2016

Data Epistemologies / Surveillance and Uncertainty

Sun Ha Hong
University of Pennsylvania, sunha.hong@gmail.com

Data Epistemologies / Surveillance and Uncertainty

Abstract

Data Epistemologies studies the changing ways in which 'knowledge' is defined, promised, problematised, legitimated vis-á-vis the advent of digital, 'big' data surveillance technologies in early twenty-first century America. As part of the period's fascination with 'new' media and 'big' data, such technologies intersect ambitious claims to better knowledge with a problematisation of uncertainty. This entanglement, I argue, results in contextual reconfigurations of what 'counts' as knowledge and who (or what) is granted authority to produce it – whether it involves proving that indiscriminate domestic surveillance prevents terrorist attacks, to arguing that machinic sensors can know us better than we can ever know ourselves.

The present work focuses on two empirical cases. The first is the 'Snowden Affair' (2013-Present): the public controversy unleashed through the leakage of vast quantities of secret material on the electronic surveillance practices of the U.S. government. The second is the 'Quantified Self' (2007-Present), a name which describes both an international community of experimenters and the wider industry built up around the use of data-driven surveillance technology for self-tracking every possible aspect of the individual 'self'. By triangulating media coverage, connoisseur communities, advertising discourse and leaked material, I examine how surveillance technologies were presented for public debate and speculation.

This dissertation is thus a critical diagnosis of the contemporary faith in 'raw' data, sensing machines and algorithmic decision-making, and of their public promotion as the next great leap towards objective knowledge. Surveillance is not only a means of totalitarian control or a technology for objective knowledge, but a collective fantasy that seeks to mobilise public support for new epistemic systems. Surveillance, as part of a broader enthusiasm for 'data-driven' societies, extends the old modern project whereby the human subject – its habits, its affects, its actions – become the ingredient, the raw material, the object, the target, for the production of truths and judgments about them by things other than themselves.

Degree Type

Dissertation

Degree Name

Doctor of Philosophy (PhD)

Graduate Group

Communication

First Advisor

Carolyn Marvin

Keywords

data, knowledge, new media, surveillance, technology, uncertainty

Subject Categories

Communication | Other Sociology | Philosophy of Science | Sociology

DATA EPISTEMOLOGIES / SURVEILLANCE AND UNCERTAINTY

Sun-ha Hong

A DISSERTATION

in

Communication

Presented to the Faculties of the University of Pennsylvania

in

Partial Fulfilment of the Requirements for the

Degree of Doctor of Philosophy

2016

Supervisor of Dissertation

_____

Carolyn Marvin, Frances Yates Professor of Communication

Graduate Group Chairperson

_____

Joseph Turow, Robert Lewis Shayon Professor of Communication

Dissertation Committee
Sharrona Pearl, Assistant Professor of Communication
Marwan Kraidy, Anthony Shadid Chair in Global Media, Politics & Culture

DATA EPISTEMOLOGIES /
SURVEILLANCE AND UNCERTAINTY

Acknowledgements.

The present work is entirely my own;
yet in everything I write lies a debt to another.
To the following, and to many others,
I present this text as my thanks.

Carolyn Marvin

Sharrona Pearl | Marwan Kraidy

Lauren Berlant | John Durham Peters

Kelly Gates | Amit Pinchevski | José van Dijck

Sandra Ristovska | Aaron Shapiro | Yoel Roth | Bo Mai

Michel Foucault | Gilles Deleuze | Maurice Merleau-Ponty

My family – past, present and future
and Jessica
for their many sacrifices

ABSTRACT

DATA EPISTEMOLOGIES / SURVEILLANCE AND UNCERTAINTY

Sun-ha Hong

Carolyn Marvin

Data Epistemologies studies the changing ways in which 'knowledge' is defined, promised, problematised, legitimated vis-à-vis the advent of digital, 'big' data surveillance technologies in early twenty-first century America. As part of the period's fascination with 'new' media and 'big' data, such technologies intersect ambitious claims to better knowledge with a problematisation of uncertainty. This entanglement, I argue, results in contextual reconfigurations of what 'counts' as knowledge and who (or what) is granted authority to produce it – whether it involves proving that indiscriminate domestic surveillance prevents terrorist attacks, to arguing that machinic sensors can know us better than we can ever know ourselves.

The present work focuses on two empirical cases. The first is the 'Snowden Affair' (2013-Present): the public controversy unleashed through the leakage

of vast quantities of secret material on the electronic surveillance practices of the U.S. government. The second is the 'Quantified Self' (2007-Present), a name which describes both an international community of experimenters and the wider industry built up around the use of data-driven surveillance technology for self-tracking every possible aspect of the individual 'self'. By triangulating media coverage, connoisseur communities, advertising discourse and leaked material, I examine how surveillance technologies were presented for public debate and speculation.

This dissertation is thus a critical diagnosis of the contemporary faith in 'raw' data, sensing machines and algorithmic decision-making, and of their public promotion as the next great leap towards objective knowledge. Surveillance is not only a means of totalitarian control or a technology for objective knowledge, but a collective fantasy that seeks to mobilise public support for new epistemic systems. Surveillance, as part of a broader enthusiasm for 'data-driven' societies, extends the old modern project whereby the human subject – its habits, its affects, its actions – become the ingredient, the raw material, the object, the target, for the production of truths and judgments *about* them by things *other* than themselves.

Table of Contents.

List of Tables and Figures.

Introduction.

Data Epistemologies studies the changing ways in which 'knowledge' is defined, promised, problematised, legitimated vis-à-vis the advent of digital, 'big' data surveillance technologies in early twenty-first century America. It analyses the entanglement of claims to knowledge and the problematisation of uncertainty: new surveillance technologies are legitimated through their promise of new epistemic potential, but these very claims equally depend on the projection of grand uncertainties (both about the world 'out there', and about the self 'in here'). Specifically, it focuses on two empirical cases. The first is the 'Snowden Affair': the public controversy unleashed through the leakage of vast quantities of secret material on the electronic surveillance practices of the U.S. government. The second is the 'Quantified Self', a name which describes both an international community of experimenters and the wider consumer technologies industry built up around the application of data-driven surveillance technology for self-tracking every possible aspect of the individual 'self'. What does it mean to 'know' about a vast, secret surveillance apparatus, even as individuals remain largely cut off from experiencing it for themselves? What kind of 'self-knowledge' is gained

through the deployment of smart sensors and tracking devices, if it is a knowledge collected and analysed at a level beyond the human sensorium? Across both contexts, I show that the hopes and fears of data-driven knowledge are founded on a pack of deferred and hypothetical techniques for knowing. Far from its dark *negation*, the uncertain and the unknown are crucial building blocks for claims to knowledge.

Surveillance and uncertainty thus constitute the central conceptual and empirical points, whose many connections define the scope of this work. Uncertainty is a familiar enough fixture in analyses of late modern societies. It appears with regularity in theories of neoliberal precarity (Gill & Pratt 2008, Giorgi 2013, Neilson & Rossiter 2008, Vadolas 2012) and cynicism (van Zoonen 2012). In information theory and its neighbours, uncertainty is typically a form of error or 'noise' – the lack of, or the opposite of, information and knowledge (Shannon & Weaver 1963; Leydesdorff 2000). Yet it is rarely taken up as a primary object of inquiry, and frequently passes without clear definition. In our context, uncertainty refers to *that which surveillance discourse admits cannot be accounted for in its system of knowledge production*. A paradigmatic example is found in state surveillance discourse: the idea that we can 'never know for sure' if we are safe from the next terrorist attack. This

uncertainty is itself repackaged into different forms to furnish partial and provisional bases for narratives, operational norms and political decisions. The allegedly unpredictable danger is thus articulated in terms of mathematical probability, or as a terrifying possibility that, given its disastrous nature, 'must' be treated *as if* real (Chapter 3). What things should be designated as what kind of uncertainty, and what attitudes should be held towards them, is subject to a constant struggle that the present work seeks to unpack.

Surveillance, meanwhile, is used as shorthand for contemporary online surveillance; that is, *digital, data-driven monitoring of human subjects for predictive purposes in the early twenty-first century*. Such surveillance often features indiscriminate and comprehensive data collection; automated and persistent monitoring; autonomous, and sometimes adaptive/learning, machines and algorithms; identification of correlations based on quantified data. In other words, the present work treats surveillance primarily as a technology of knowledge production, rather than instrument of control or technological invention. To be sure, the latter remains a framing concern. My analysis is built on top of recent scholarship on the social meaning of code, algorithm and data, including the idea of surveillance as 'social sorting' (e.g.

Bauman & Lyon 2013; Gandy 1993; Lessig 2006; Mackenzie 2006; Poster 1995); on surveillance as control, discipline, 'securitisation' and criminalisation (e.g. Deleuze 1992; Foucault 1995; Mattelart 2010); critiques of surveillance vis-à-vis privacy (e.g. Bogard 1996; Cohen 2013; Diffie & Landau 1999; Zimmer 2008); and existing studies into data-driven surveillance in contexts like airport security and biometrics (e.g. Aas 2006; Adey 2009; Amoore 2009; Gates 2011; Parks 2007). The focus in these pages, however, is squarely on the *epistemic* stakes and consequences of electronic surveillance.

***

Such surveillance is nevertheless too wide a field to survey. New techniques for extraction and analysis of personal data affected a diverse array of practices during the early twenty-first century – from social media platforms to crowdsourced scientific work, from biometric surveillance at airports to e-mail metadata collections, from prosthetic sleep quality trackers to 'smart' lights embedded in home furnishings. The present work focuses on two specific developments, and the debates accompanying them: the Snowden Affair, and the Quantified Self.

In June 2013, Edward Snowden, contracted by proxy to the National Security Administration [NSA], fled the United States with a vast cache of secret documents that detailed telecommunications surveillance systems operated by the NSA, and sometimes the FBI and the CIA, against both foreign and domestic populations. The leaks made an instant impact, launching a lengthy public debate over the virtues of electronic surveillance. Although vague warnings and suspicions had previously accompanied the American government's expansion of surveillance operations following the September 11 terrorist attacks in 2001, the Snowden files was more or less the first to provide concrete and comprehensive evidence[1] pointing to activities widely thought to be illegal – from the bulk collection of telephone and e-mail metadata from domestic populations, to secretly 'tapping' undersea data cables to harvest personal information on online activity. Over the next several months, Snowden, or rather, the journalists to whom he delegated the task, revealed information that claimed to show that the NSA had spied on foreign diplomats and national leaders; that they had monitored players of online video games; and even surveilled pornography consumption habits as

[1] As we will see in Chapter 3, many parts of the NSA's surveillance programs had been revealed in a series of exposés during the preceding decade, featuring whistleblowers and insider sources such as William Binney, a 30-year veteran of the NSA, and Mark Klein, then a technician for the telecommunications company AT&T. However, these whistles blown earlier failed to maintain visibility beyond a few days or weeks of the news cycle – perhaps because of the absence of 'material' proof like the Snowden files.

blackmail fodder against 'radicalisers'. The ensuing debate would lead to numerous government reviews, court cases filed by civil rights organisations, and, to date, one piece of legislation – the USA Freedom Act.

The analysis of the Snowden Affair primarily addresses the two years following the first leaks (2013-2015), and the public debates over the extent and legitimacy of state surveillance programs across the courts and Congress, news media of various stripes, even documentaries and fiction. At the same time, the Affair – and the surveillance systems it exposed – had a long tail stretching back at least to the beginning of the century.[2] In the late 1990s, the NSA was struggling to assert its significance – and retain its old levels of funding – in the post-Cold War era. Its leadership, burned by Watergate, had maintained a policy of caution when it came to domestic surveillance (e.g. Bamford 2008, p27). September 11, and the George W. Bush administration's response to it,[3] kickstarted a dramatic expansion in state surveillance

[2] To be sure, the history of electronic communications surveillance by the US government goes back almost as far as the history of electronic communications themselves – including Herbert Yardley's 'The Black Chamber' of the 1920s. But the specific surveillance systems leaked by Edward Snowden were an outcome of the political climate following the September 11 terrorist attacks.

[3] Following September 11, President Bush, and Vice President Dick Cheney immediately moved to produce a legal basis for vast expansion in domestic surveillance powers. This was provided by David Addington, the ultra-hawkish legal counsel to Cheney, and the Office of Legal Counsel, in what eventually became the "Authorisation for specified electronic activities during a limited period to detect and prevent acts of terrorism within the United States". This memo was so secret that only several persons within the NSA could access it.

capacities that would culminate in the wide array of programs, from PRISM to XKEYSCORE to BOUNDLESS INFORMANT, that Edward Snowden would expose. This expansion, in many ways, wholly embraced networked computing technologies and the epistemological faith in 'big' data, resulting in a certain data hunger: as one anonymous intelligence official described, "let's collect the whole haystack […] collect it all, tag it, store it… and whatever it is you want, you go searching for it." (Nakashima & Warrick 2013) This broader background of counter-terrorism and surveillance discourses throughout the early twenty-first century shapes the present analysis of the Snowden Affair.

Beyond the state and terrorism, a similar set of technologies and epistemic principles were being spun around very different stakes and environments. If the Snowden Affair was a belated public contestation over surveillance systems already deployed nationwide, *self-surveillance* names practices of everyday, 'lifestyle' tracking that remains, at time of writing, an emerging and still experimental mixture of real devices and fantastic promises. These

---

Until the Snowden leaks in 2013, the legal justification for the programs then migrated across variously secret forms of legislation, including a 2004 opinion by the Foreign Intelligence Surveillance Court [FISC] judge Colleen Kollar-Kotelly (itself secret), and then the 2008 FISA Amendments Act (during which period most members of Congress were denied clear information on how the legal provisions were being operationalised vis-à-vis American citizens). For more, see (Mayer 2006; *PBS Frontline* 2014).

technologies were designed to datafy aspects of the self that has traditionally escaped mechanisms for self-knowledge. By the mid-2010s, mass produced devices were promising to provide accurate, objective knowledge about sleep quality, mood fluctuations, steps taken, stress levels, average duration of sexual intercourse, and more – all through increasingly miniature and automated devices that would live on the skin and/or in the home, silently and constantly *tracking* their human owners.

This kind of self-tracking is stretched across a number of popular labels and industry clusters, producing rather porous boundaries. Many self-trackers are also 'wearables' – typically sensor-equipped devices worn on the body – but not all wearables are primarily built for self-knowledge. Many belong to the broader paradigm of an 'Internet of Things', a wider vision of exhaustively connected object environments that includes infrastructural deployments like 'smart' electricity meters. Here, I focus on personal devices and programs that stick to the users' bodies and homes, and thereby produce formalised knowledge about their everyday lives – thereby aligning with the above definition of surveillance.[4] The archetypical device, and one which played a

[4] This demarcation is broadly in agreement with the small but growing scholarly literature on self-tracking / the Quantified Self. For instance, Melanie Swan defines QS as "any individual engaged in the self-tracking of any kind of biological, physical, behavioural, or environmental information" (2013, p85).

leading role in popularising the concept of self-tracking to the wider American public, is Fitbit; a fitness tracking wristband which automatically collects physiological signals and delivers quantified analytics on one's health and exercise. Founded in 2007, Fitbit released its first iteration in 2009 – and by 2015, was boasting 1.86 billion USD in revenue (*Fitbit* 2016).

Within the self-tracking landscape, the present work addresses two distinct but overlapping groups. The first is the self-tracking industry in general, which has grown from a smattering of prototypes in the mid-2000s to a consumer market that is still immature, but able to boast giants like Fitbit. In many cases, this industry developed through translations of technology and technological ambitions across academic science, industry R&D and existing commercial applications of machinic sensors and data analytics. Beddit, a sleep quality tracking device, was conceptualised during founder Lasse Leppäkorpi's academic research into ballistocardiography; he and his team would turn the technology first to application in hospitals and luxury bedding companies, before raising funds through venture capital and online crowdfunding to produce the self-tracking device. Muse, a headset for tracking and augmenting meditation activity, is built on electroencephalography [EEG], one of the most common methods in early

twenty-first century neuroscientific research. The development of the device was spearheaded by Ariel Garten – an artist-cum-fashion designer-cum-entrepreneur who had at one point worked with Steve Mann, the pioneering figure in the history of wearable computing (see Hansen 2014). Self-tracking industries thus brokered one channel for the popularisation of data-driven surveillance for personal use. To be sure, the exact size and characteristics of this market is difficult to gauge; industry metrics for sales and revenue are still disorganised, often folded into different categories like wearables (See Chapter 2 for more). Ultimately, it is beyond the scope of this dissertation to assess the 'success' of self-tracking as a consumer good. As a product of its own temporal moment, this work treats self-tracking as an emerging cultural practice, and self-tracking discourse not as representations of an already enacted reality but futurist visions intended to mobilise the public towards new sociotechnical systems.

Alongside this wider industry is the Quantified Self [QS] community – a decentralised network of early adopters, hackers, experimenters. QS was founded in 2007 by Gary Wolf and Kevin Kelly, two veterans of the technology magazine *Wired,* for discussing the potential of new technologies for quantifying and knowing the self. Following their inaugural offline

'meetup' in San Francisco – where some twenty-five individuals showed up – Wolf and Kelly invited those interested to organise and host local meetups wherever they liked; by 2015, QS boasted locally organised meetups across every continent on Earth and bi-annual conferences in America and Europe. QS is best understood as a community of practically oriented enthusiasts, united by the belief that new technologies can be used to deliver better self-knowledge and thereby well-being and happiness. QS meetups emphasised personal 'show and tell's; short narratives of personal experimentation about how one hacked a Fitbit to track one's exercise patterns more accurately, or developed a simple set of spreadsheets customised for one's particular responsivity to diabetes. Gary Wolf's unofficial guidelines (2010) recommended avoiding not only 'business pitches', but 'general philosophical / speculative discussion' – a way to focus on specific experiments for practical benefits. With all this in mind, the relationship between QS and the wider industry might be parsed in terms of Pierre Bourdieu's categories of connoisseur and layman, originally applied to the fields of sport (e.g. 1984, 1991): a smaller group of dedicated insiders who develop a communally specific set of competencies and 'schemes of perception', whose articulated values and principles trickle out – in many distorted forms – to a wider and sporadically involved public. The connoisseur community of the Quantified

Self was a space for tech geeks, entrepreneurs, health industry professionals, journalists and self-care enthusiasts to cultivate social norms for talking and thinking about the future of self-surveillance.

In many ways, QS' model of an informal tinkerers' community took after similar connoisseur groups in the early days of personal computing, such as the now-famous Homebrew Computer Club of the 1970s and 80s.[5] The similarity was not coincidental. Kevin Kelly, fifty-five years old by QS' founding, had been what Fred Turner (2006) calls a 'network entrepreneur'; an individual who brokers connections across different social groups to build wider enthusiasm for a collective vision. Kelly was an integral part of three seminal mediums – the Whole Earth Network, the WELL, and *Wired* – that proselytised a utopian vision of personal computing and human augmentation in the latter half of the 20th century. Gary Wolf, belonging to a younger generation, had entered the field as a consumer of the WELL online community, subsequently working as a contributing editor at *Wired* for over twenty years (see Medosch 1997). This heritage, as we will see in Chapters 2

[5] In 2011, Gary Wolf referred to QS as a 'users group': "informal but deeply engaged learning communities operating outside the normal channels of academic and commercial authority" (Boesel 2013). It is clear that QS was envisioned by its founders to be a haven for free-spirited amateurism, even as many of its participants make use of and are involved in developing commercial self-tracking products.

and 4, would be played up to present self-tracking as part of a broader trajectory of technological progress towards objective knowledge.

One immediate consequence of this 'looser' structure is that the exact size and composition of QS difficult to pin down. Estimates of 'members', based on local meetup sizes[6], ranges from 2,500 in March 2011 (Kelly 2011), to 5,000 across some seventy local meetups in 2012 (Swan 2012). The only systematic account of QS' size and growth comes from Adam Butterfield (2012), then a graduate student in Applied Anthropology. His report identified around 4,800 members within the U.S. as of 2012, distributed across local meetups in 27 locations, from Fort Lauderdale to New York City. Here, I treat QS as a group of dedicated amateurs, yet one whose personnel and practices overlap greatly with the commercial and marketing interests of the industry; a rapidly growing community with a strong media presence, but a distinct minority relative to the tens of millions of wearables purchasers across the United States. My analysis of self-surveillance draws from both groups – often

[6] The very label 'members' is problematic, since QSers are not card-carrying members organised through, say, subscriptions to services or regularly paid dues. These metrics of 'members' are likely to refer to records of meetup attendance, and/or informal registrations of interest/attendance at such meetups. I refer to anybody involved in QS' various events without disavowing their relationship with the community, as well as individuals who explicitly relate themselves to QS, as a 'QSer'.

identifying discourses and ideas common to both, and sometimes parsing the differences between the two (and within each one).

These two manifestations of surveillance technology remain underconnected, especially in popular discourse. Self-tracking is rarely described as surveillance, and instead tends to be buoyed by narratives of empowerment, individualisation and self-optimisation. Accordingly, if discussions of state surveillance is dominated by fears over privacy and control, those same issues tend to be glossed over either as secondary concerns for the future – or as a small price to pay for advancements in self-knowledge. Yet both types of knowledge production are rooted in common technological capacities and principles, from automated data collection to the constant hunger for 'bigger' data. Along with corporate data-mining, wherein individuals' consumption activity is processed into digital profiles and monetised, state and self-surveillance constitute major sites for the emergence of data-driven knowledge regimes in early twenty-first century America.

'Emergence' – because these technologies are still immature, and the moral, institutional and narrative foils for their normalisation are still forming in contingent ways. The present work analyses the Snowden Affair and the

Quantified Self precisely because they are two places where such emergent processes are most visible. In the former, state surveillance is challenged in the most openly public way; in the latter, self-surveillance bullishly asserts its own legitimacy – even as it is, as we shall see, being colonised by corporate interests. They are thus places and moments where the epistemic fantasies of new surveillance technologies are being openly debated, asserted, defended. Across both state and self-surveillance, the present work asks: what kinds of stories are being told about technology and knowledge? Where do these stories go to defend themselves, to what values and narratives do they fall back on? What we find is the resuscitation of the oldest tricks in modernity's book (our enduring fixation with objectivity and calculability), wrapped up in narratives of novelty (of new terrorist threats, new machinic capabilities). The constant modulation of knowledge and uncertainty, derived into many subsidiary narratives of security, transparency, optimisation, freedom. Over the next four chapters, I present two seemingly discrete quests for data-driven; cases which, when triangulated, depict the diverse ways in which the political, cultural, technological, material, economic efforts of the 'new media' society are being directed towards the glowing promise of data as knowledge, machines as knowledge.

METHODS AND AIMS

The present analysis draws on research into the public presentation of surveillance vis-à-vis the Snowden Affair and the rise of self-tracking technologies, with a focus on the United States. By public presentation, I mean the ways in which surveillance was made object of debate, description, speculation, criticism – through media discourse, through the commercial introduction of technological solutions, through local community gatherings and nationwide conferences. My use of 'public' thus aligns with what has been called 'publicly oriented' (Warner 2002) or 'publicised' (Habermas 1991): discourse intended for, and circulated to, a wider community of indefinite strangers. This work does not seek to explain what 'really' happens under the hood with surveillance technologies, nor to discover how American citizens 'really' respond to these technologies in their private thoughts and lives. Instead, it describes what visions of surveillance societies are presented in mediated, publicised discourse. It seeks to understand what kinds of attitudes to uncertainty are being sold to the public as normal, natural, useful, necessary.

The present work draws on three years of research (2014-2016) across a wide variety of sources to sketch out the character of this publicised discourse. In

the case of the Snowden Affair, this meant examining the primary scenes of public contestation over the implications of the leaked information. Media coverage from a selection of prominent news publications were collected, classified and analysed. The selection sought reputable, prominent, high-circulation publications with a variety of political biases, namely: *National Review, The New Yorker, The Atlantic, The New York Times, The Washington Post, The Weekly Standard, Wired* (online, and print where applicable). Additionally, I examined coverage in *The Intercept,* founded in direct response to the Snowden Affair and featuring Glenn Greenwald and Laura Poitras as editors. *The Guardian* (online) is also included, given its critical role in the Snowden Affair and the fact that it is widely read by U.S. readers (which is not true of *Der Spiegel*). Hence the scope of the sample is delimited by readership and influence, rather than institutions' headquarters. From this selection, a pool of over 1,000 articles were extracted, then further sorted for items focusing on the themes of uncertainty, secrecy and proof relatively directly. This corpus was triangulated with speeches and official statements from actors in the U.S. government, including addresses by President Barack Obama and successive Directors of the NSA, Michael Hayden and Keith Alexander. The actual material leaked by Edward Snowden was also extensively consulted, sourced from major online archives like LeakSource, the Snowden Surveillance

Archive and Cryptome – as well as public appearances by Snowden and his 'accomplices', Glenn Greenwald and Laura Poitras.

For self-surveillance, the complex landscape of the Quantified Self community and self-tracking *tout court* necessitated a broader set of inquiries. First, media coverage of self-tracking was collected and analysed as with state surveillance. Here, the selected publications included more general ones like *The New York Times,* as well as major publications in the technology industries and computing culture spaces such as *Wired* and *Fast Company*.[7] Second, I examined approximately fifty self-trackers on the market or in prototype stage, including their provenance (their creators, sources of funding, route to development), marketing discourse (in product websites, interviews, crowdfunding campaigns, and so on) and the tracking devices themselves. This was supplemented by research into the various online and offline presence of the QS community. This included the full archives of the Quantified Self website – maintained by Wolf, Kelly and a small number of collaborators – which serves as a hub for networking different self-tracking products, experiments and trends as well as disseminating information about

[7] The full list of publications are as follows: *The Atlantic, Fast Company, Harvard Business Review, Inc., National Review, The New York Times, The New Yorker, The Washington Post, Wired.*

the QS community. I also held site visits in three meetups across New York and Philadelphia, each involving between ten and fifty participants, and analysed over a hundred QS 'show and tell' sessions uploaded online by the community. I conducted four interviews with QSers of varying types of involvement. This included Gary Wolf, the co-founder of QS and a key figure in evangelising, framing and networking self-tracking practices across tech communities, scholars, industry actors and the wider public; and Chris Dancy, a self-tracking entrepreneur and experimenter whose practices once earned him the moniker 'the most connected man on earth'. Finally, I attended the 2015 Quantified Self Conference in San Francisco, where I was able to observe over forty panels, workshops and product showcases. These various scenes constitute a robust cross-section of the different ways in which self-tracking is made present for public consumption in the United States.

***

The next four chapters each highlight a specific relationship between knowledge and uncertainty, focusing either on state surveillance and the Snowden Affair (Chapters 1, 3) or self-surveillance and the Quantified Self (2, 4). Chapter 1 examines the layers of evidentiary politics surrounding the

Snowden Affair – a controversy where the state insists 'bulk' surveillance is necessitated by a radical evolution of unpredictable terrorism, and where the whistleblower's dramatic revelation of secret truths provoked waves of speculation and uncertainty. What counts as 'proof'? What does it mean to know 'about' a vast surveillance system one can rarely experience directly – or ever know in its fullness? To navigate this terrain, Chapter 1 traces what it calls *recessive objects*: objects which promise to extend our knowability, but thereby publicises the very uncertainty that threatens the claims to knowledge. Two such objects are examined: the evidentiary archive that is the Snowden files, and the 'lone wolf' terrorist as a figure of analysis and speculation. Turning to self-surveillance, Chapter 2 focuses on the claims surrounding *machinic sensibility:* the capacity of 'smart' machines to collect and analyse the kinds of data that are fundamentally unavailable to human subjects. Self-tracking thus positions human cognition, intuition, experience, as the wellspring of uncertainty – which it promises to eliminate through new technologies. The corollary is that in its efforts to 'bypass' the human subject and retrieve objective data, self-surveillance offers the kind of 'self-knowledge' that is structurally black-boxed out of the users' ability to know.

Having sketched out the lurking presence of uncertainty and its bedfellows (the unknown, the unpredictable, the secret…) vis-à-vis data-driven surveillance, the latter two chapters (3, 4) focus on how claims to knowledge are nevertheless constructed and defended. Chapter 3 examines how, in the face of 'New Terrorism', claims to knowledge are secured through a set of techniques for simulated and deferred knowing. They include *subjunctivity*, wherein it is argued that decisions must be made 'as if' the unknown is known, 'as if' the hypothesis is proven; *interpassivity*, where the ignorance of the public or other subjects is compensated by the hypothetical Other who knows in their stead; and *zero-degree risk,* where uncertainties' resistance to traditional means for calculating risk produces a more naked turn towards a 'just-in-case' politics: we must watch everyone, no matter the probability. Lastly, Chapter 4 analyses how self-surveillance exhorts its users to develop *data-senses* in a posthumanist adaptation to new knowledge technologies. It argues that self-tracking's claim to transformation in self-knowledge is undergirded by a *honeymoon objectivity*: the reprisal of old, modernist faiths in linear, technological progress and absolutely objective truth, carried by the mythic material of 'raw data'.

'RAW DATA'

Across it all, 'data' is the object which embodies – an ironic expression, since so much of what is invested in it is potential, fictional, speculative – the epistemic fantasies of new surveillance technologies. Data is the indispensable unit at the heart of the assumed process whereby real phenomena – the threats of lone terrorists, the sprawling state surveillance apparatus, the goldilocks correlations that can optimise the self – might be formalised into reliable, solid, pieces of information. After all, without such raw ingredients – anterior to human meaning, and amenable to computation – how could one claim the superiority of machinic sensibility in epistemic endeavours?

Raw data typically refers to data generated by the machine, but not yet having undergone 'secondary' processes of statistical analysis, cleaning, visualisation, aggregation, and so on. In short, data fresh out of the sensor. In this telling, raw data is untreated, unprocessed; it is seemingly anterior to analysis, classification, the attribution of *meaning*. Of course, to even call it 'raw data' is redundant; 'data' itself refers literally to 'the givens'. Today, it is a term that so often is accepted without question; a thing whose relationship to objective inquiry and observation simply dips under the radar, becoming "something we would *not* want to deconstruct" (Rosenberg 2013, p18). This

belief in raw data's *non-mediated nature* is crucial to new surveillance technologies' claims to accessing objective reality. In other words, it is precisely because data can be collected 'raw' that it can be said to impartially or neutrally extract from reality, from *noumena.* Raw data provides a concrete object, a presence, for the theoretical availability of objective self-knowledge. Consider the role it plays in discourses of self-surveillance. At meetups and conferences, Quantified Selfers reviewing each other's experiments can be found constantly asking: where is the raw data? In 2015, one QSer suggested raw data access as one of the three 'freedoms of personal data rights':

> Without raw data, we are captive to the 'interface' to data that a data holder provides. Raw data is the 'source code' underlying this experience. Access to raw data is fundamental to giving us the freedom to use our data in other ways (Ramirez 2015).

Similar sentiments were expressed by a host of influential commentators, including QS co-founder Gary Wolf (e.g. Wolf 2016; Watson 2013). The valorisation of raw data is intimately connected to self-tracking's vision of personalised control; data, self-trackers insist, must not be 'siloed', 'hidden', made 'passive'. The irony is that at the same time, raw data is commonly understood to be opaque, even incomprehensible:

> 'People aren't really interested in raw data,' Chang says. 'If I just gave you your heart rate data, you wouldn't know how to interpret it. In fact, it might confuse you, or it might scare you and say, 'What is the spike? Why is it low? Why is it high?'' (Shahani 2012)
>
> We have algorithms to break down everything. Because the raw data collected on the device doesn't really mean anything, it's the firmware and the software, with its intelligent algorithms that help explain what a movement was (Creasey 2014).

Such discursive appearances exemplify a double-bind at the heart of surveillance's epistemic promise. Data's 'rawness' allows it to claim a representational purity – even as that 'rawness' restricts the data's legibility to human sensibility. Self-trackers' search for raw data, and the valorisation of access to raw data, thus mirrors the 'data hunger' witnessed in state surveillance systems: an archival fever (Derrida 1998) that seeks an orderly and complete accounting of natural phenomena into the ingredients of epistemology.[8]

Such discourse consistently conjures the figure of raw data as the material proof of machinic objectivity. And yet, as Lisa Gitelman and Virginia Jackson (2013) put it, 'raw data is an oxymoron'. Every piece of data is the product of a sociotechnical system; if data-sense speaks of machines recalibrating

[8] For an earlier historical episode in the *database* as a locus of epistemic desire, see Rebecca Lemov's *Database of Dreams* (2015).

humans' sensory equipment, it is humans that must calibrate those machines in the first place.[9] Data is always the product of a mediative frame, and its presentation as unadorned information is always vulnerable to such 'contagion' (Murphie 2015; also see Schwarz 2015). Indeed, every type of data has historically required a socialising process where its veridical authority is constructed and naturalised. One clear precedent for new surveillance technologies' claims of advancements in machinic knowledge is the late 19th century gramophone/phonograph. As chronicled by Friedrich Kittler (1986), the phonograph heralded the privileging of auditory data over articulation; a mechanical division and reorganisation of sound into a data structure entirely indifferent to the phenomenological structure, one which 'listens' to noise *regardless of meaning*. Today, the same kind of transformation is being staged through 'deep learning' – a process of machine learning which seeks to minimise manual, human specifications of *meaning*, and instead let machines break up its object (say, an image) into literally meaningless pieces to record,

[9] This point is particularly visible in contemporaneous concerns over 'algorithmic discrimination'. As automated, algorithm-driven *decision-making* became commonplace in systems ranging from identification of terror suspects in airport security (Amoore & Hall 2009) to visibility and voice in social media publics (Bucher 2012; Gillespie 2014) and the pricing of consumer goods (Kirchner 2015), the corporations controlling those algorithms have tended to default to the argument that a machine is incapable of racist and other forms of discrimination, and every perceived injustice is merely a random error within a neutral system. Yet it is increasingly clear such claims to neutrality serve to conceal and empower the humans and human decisions that undergird every such (often proprietary, black-boxed) technology (also see Gillespie 2010).

correlate and analyse.[10] Deep learning thus brings a machinic, literally inhuman sensibility to knowledge production processes in areas like video surveillance and analysis of self-tracking data. Yet the epistemic process does not end there; if it did, there would be little left that is meaningful for human subjects. Kittler shows how the fragmentation of human experience into dividual bits is followed by a reconstitution of such machine-produced data into an effect of the real – the emblematic technology here being cinema. The ability to claim 'rawness' is thus nothing more or less than a historical belief in a given technological process as a privileged ambassador for objectivity. 'Raw data' is very far from knowledge or meaning; the sociotechnical treatment of that data matters far more than any illusion of pristine information.

***

[10] For instance, a deep learning system assigned to 'recognise' photographs' content will not begin with manual designations, where the programmer might assign a certain constellation of pixels as 'ears' or 'bugs' *before* the machine begins to see. Instead, a given neural network might be assigned a vast set of images to analyse – and each time, also presented with the 'correct' answer that it would gradually modify itself to match. This is why, as artist duo Shinseungback Kimyounghun (2012; 2013) show, deep learning machines will see human faces in clouds and cat faces in humans; the 'face' has no meaning as a face, only a particular (and, clearly, imperfect) correlation of bits of visual data. This *ignorance* of the computer, which allows it to truly *learn* rather than copy or memorise, replicates the Enlightenment's invention of the 'innocent' observer as a nonsubjective and thus truly scientific subject (Picciotto *in* Gitelman & Jackson 2013, p4-5).

All in all, Data Epistemologies is a critical diagnosis of the contemporary faith in 'raw' data, sensing machines and algorithmic decision-making, and of their public promotion as the next great leap towards objective knowledge. Within the contexts of state and self-surveillance, it seeks to understand how surveillance technologies' claim to knowledge are constructed; how those claims depend on the projection of vast uncertainties, and themselves often produce new relationships of uncertainty; and how fantasies of objective truth, technology as unbounded progress and the 'rawness' of data are synergised to endow these claims with legitimacy.

In many ways, this means that the analysis is a product of and for the present moment – a moment of what we still call 'new' media technologies. The phenomena in question are very much contemporary, and their consequences are yet to be played out in full. Many of the legal and political contestations provoked by the Snowden leaks remain in progress. While the USA Freedom Act of 2015 promised to reform the state surveillance apparatus, its actual impact fell far short of the name.[11] Meanwhile, the narrative of New Terrorism

[11] Having prohibited one specific legal interpretation (Section 215) that had allowed bulk collection of telephone metadata from American sources, and enacted several other reforms, the Act left almost untouched vast areas of the state surveillance apparatus created or expanded during the post-September 11 era. For instance, the interception of 'foreign' Internet communications which, due to the ways in which data infrastructure has been

retains its rhetorical efficacy, maintaining the discursive landscape that pitches the vision of national security under threat against the advocates of privacy and civil rights. Self-tracking technologies are at the infancy of their life as mass-produced, mass-consumed devices. Data Epistemologies addresses the scholarly and public debates accompanying these formative developments – debates which typically parse surveillance in terms of political power and technological advancement, with a corresponding focus on objective proof, transparency of information, and the violation of rights. By focusing on the organisation of epistemic definitions, legitimacy and problems in the surveillance context, it offers an alternative, and complementary, analysis of the basic *ground* for political struggle and consensus that surveillance discourse is working to establish.

The present work also speaks to a number of broader contexts for debate and scholarship. First, it provides a sustained analysis of uncertainty vis-à-vis knowledge and surveillance. Although uncertainty is often identified as a key characteristic of late modern life (e.g. Giddens 1990), it is rarely subject to focused, sustained and empirical analysis. Alongside broader theses about,

---

constructed over previous decades, continues to collect vast amounts of domestic communications as well.

say, the 'persistent existential anxiety' of the modern subject (ibid., p98-100), the concept of *risk* has often attempted to take more specific account of how modern societies manage and contain uncertainties. Yet figures like the definitionally unpredictable lone wolf terrorist and the fantasy of 'big' data as absolutely comprehensive knowledge show that uncertainty as an object for thought and action cannot be fully contained by risk, or other systems of knowing (Chapter 3). In the context of new surveillance technologies, I argue that uncertainty is consistently produced as the necessary counterpart of claims to knowledge – such that to invoke one is to thereby manage the other. If the typical modern narrative depicts the colonisation of the unknown through reason, or at least its management through probabilistic calculation, this is a story of the ouroboros, the serpent that devours its own tail: claims of knowledge and uncertainty locked in constant cannibalism, defining each in the context of the other.

The analysis of surveillance in the Snowden Affair and the Quantified Self also relates more generally to how we think about technology, knowledge and truth. Data Epistemologies intersects two matters of concern: the constructed ideas of objectivity and reason, and the visions of technological transformation that surround the expanding reach of digital technologies.

(Indeed, the very fact that we have used the name 'new media' for over twenty years is an indication of this continually replenished image of progress and revolution.) Digital surveillance's claim to significance thus leverages far older and broader ideals, often wound tightly around the most fundamental aspects of our lexicon: information, proof, secret, objectivity, technology, data. The fantasies of technological transcendence, of perfect proof, of 'raw' data, of unerring machines… behind all of these lie the constant flux of veridical authority and epistemic structures, the many negotiations and skirmishes over what should count as knowledge, as unknowable, as 'sufficiently' known, as necessary to know.

1. Recessive Objects.

The Snowden Affair exhibits a curious parallelism. If the state pleads the necessity of total surveillance to capture unpredictable terrorists, the whistleblower asserts the necessity of transparency to uncover the abuses of surveillance. Even as NSA analysts speak of 'analysis paralysis'[12], buried in 'big data' too big to render meaningful, the public is itself confronted by leaked information of massive proportions. These problems cut deeply into traditional axiologies of secrecy and publicity, knowledge and ignorance. This chapter examines surveillance's claims to knowledge – and critics' claims to knowledge *of* surveillance – and their dependency on visibilising the uncertain and unknown. It studies the politics of who claims to know for whom, what is marked out as knowable (or not), what kinds of knowledge are established to be necessary (for our security, our liberty). In doing so, I raise the concept of *recessive objects*: objects which promise to extend our knowledge, but thereby publicise the very uncertainty that threatens knowability. These ambivalent objects – the Snowden files, and the lone wolf

[12] Internal NSA memos leaked by Edward Snowden (see Maass 2015) speak of 'analysis paralysis' and 'too many choices'; some were even titled "Data is Not Intelligence" and "In Praise of Not Knowing".

terrorist – bring into social presence the struggles over what counts as knowledge and how.

***

The website of *The Guardian* blinked, refreshed. "NSA collecting phone records of millions of Verizon customers daily," read the headline (Greenwald 2013a). The same day, the 6th of June, 2013, the print edition followed suit: "US orders phone firm to hand over data on millions of calls" (Greenwald 2013b). *The Washington Post* joined the fray with online and print pieces over the next 48 hours. The thing about news is, of course, that so much of it is ever so familiar – novelty and repetition in guise of each other.[13] These reports of 'breaking news' featured many of the same discursive patterns found in previous post-9/11 revelations of surveillance. In 2002, Americans had already been warned about "a virtual, centralised grand database", and given a beginner's guide to the term 'data-mining'. In 2006, they were told about domestic surveillance that is so secret the public can't even be told why it is secret (*The New York Times* 2006; Page 2006), including, word for word,

[13] Guy Debord (1990) understood well that the more novelty is mass produced, the more such novelty depends on an amnesiac repetition.

"phone call records of tens of millions of Americans" (Cauley 2006). Change the names, and you might well have copied half of the story off the archives. And yet, it was presented as a revelation with seismic consequences. Sceptical quotation marks framed that now-tainted word, 'metadata': whether the reader knew what it really is (and entails) or not, they were alerted to a certain sense of secrecy and duplicity. All of these would multiply in the coming weeks and months, the repetitions sedimenting imaginations about state surveillance and 'Big Brother'.

From what concrete, material evidence did these reports derive their authority? *The Guardian* had a rare scoop: the online article provided a copy of the Foreign Intelligence Surveillance Court [FISC] order that addressed Verizon by name and demanded 'telephony metadata' (*The Guardian* 2013). The slightly grainy text, a mysterious stamp-mark reading '13-80', and the watermark TOP SECRET//SI//NOFORN [No Foreigners] attested to the materiality, secrecy, and (as if this followed naturally) authenticity of this document. Such documents would soon flood the mediascape: slides upon slides, partly blacked out reports and memos, and of course, the figure of Edward Snowden himself.

Surely, then, the story of the Snowden Affair is one of leaks and revelations: a clear case where the public becomes 'better informed', and dark secrets turn into open facts. Snowden himself had defined his "sole motive" to be "infor[ming] the public" (Gellman et al. 2013); six months after the leaks, he declared his mission accomplished, the mission "to give society a chance to determine if it should change itself" (Gellman 2013). William Binney, a former NSA employee who had told the public much the same things Snowden did with much less impact, thought the documents made the difference: he now regrets that he didn't take documents himself, the 'hard evidence [that] would have been invaluable' (Loewenstein 2014). Yet these documents were also occasions for occlusion, withdrawal, speculation, simulation. Snowden's documents, despite – or rather, thanks to – their enormous volume and scope, make present surveillance as an uncertain and unknown world. This fixation with uncertainty was not mere background. The depiction of surveillance as a grand epistemological technology for our times, whether beneficent or perfidious, was achieved precisely through relentless reference to unknowns that cannot, by definition, be completely eliminated. It is this entanglement between surveillance as knowledge production and the unknowns surrounding surveillance as practice that this chapter traces. What our age has called 'new' media has erected its own conventions for producing and

circulating knowledge – conventions which were so often endowed with the honeymoon glow of novelty and progress. This dissertation is occasion to critically examine the uncertainties produced as part of this epistemic vision, taking for this chapter the case of state surveillance dragnets.

This focus points us towards the public presentation of surveillance. What we seek here is neither the depth of a secret techno-political reality (how does surveillance 'really' work?) nor the depth of the public's psychic interior (how do people 'really' feel about it?), but what Foucault (1972, p229) called the 'surface' of discourse: how surveillance has been positioned and problematised in public, for 'the' public, in the public activity of words and things. Neither is such surface to be dismissed as the fantasies of the misinformed. It is my argument that the co-dependency of knowledge and uncertainty is not reducible to explanations at the level of ignorance, obfuscation or even secrecy – although all of those things do feature prominently. Rather, this relationship is foundational to the political emergence of indiscriminate, 'dragnet'-style surveillance in the early 21st century. Post-9/11 American state surveillance – which is merely the leader of a more international trend that includes, at the very least, British and German intelligence agencies – was founded on the rationale that terrorism had

become radically unpredictable, and so *anyone and everyone* must be watched in order to produce reliable information about its threat: a narrative which I shorthand here as 'New Terrorism'.[14] As early as 2002, the Total Information Awareness program, a precursor to the NSA programs revealed by Edward Snowden, was trying to 'connect the dots' – in one case, literally connecting the dots on a massive graph on the wall. Just to complete the joke, they called it BAG – Big Ass Graph (Harris 2010). Which other terrorists was a given suspect communicating with? How many times did a given word appear in a conversation? This visualisation of the turn to 'big' data often produced lines "so dense as to be indecipherable" to the human eye (ibid., p209).

In other words, the uncertainty generated by New Terrorism is directly linked to how the collection of everything produces its own uncertain kind of epistemology. By the time of Snowden's revelations, we find this paradox in full bloom. Under General Keith Alexander's directive (2005-2014), the NSA's vision was not just to look for the needle in the haystack, but "collect the

[14] The epistemic and political linkage between anxieties of proliferation and the dream of totalising archives, of course, is one which gained general import over the 18th and 19th centuries. One of the major narratives in Foucault's work on criminality is how Western societies shift from *inquiry* (of an event, what happened, a reprisal of the singular) to *examination*: not 'was this done? Who did it?' but "presence or absence, of existence or nonexistence … ordered around the norm" – that is, the whole curve of normality, over time as well as over space of bodies (Davidson 2004, xxiii). In the latter model, the entire curve of the population, the normals as well as abnormals, must be modelled in order to properly identify the pathological (e.g. Hacking 1990).

whole haystack" (Nakashima & Warrick 2013; also see Greenwald 2014, p96) – a reasoning replicated in internal NSA communications (Maass 2015). In crude terms, the whole point of the 'collect 'em all' strategy is that you don't know what you're looking for until you already have it, so you must always have, standing in reserve, everything you can manage to collect (McQuillan 2015).

This explicit mobilisation of the unknown as a building block for knowledge claims was a strategy replicated across both critics and defenders of American state surveillance. In early 2014, Edward Snowden and James Clapper, the US Director of National Intelligence, hit off an unintended symmetry in their public statements:

> You're giving up your rights. Your rights matter because you never know when you'll need them. People should be able to pick up the phone and call their family, should be able to send a text message to their loved one, buy a book online, without worrying how this could look to a government possibly years in the future. (Snowden *in* Rowan 2014)

> Clapper compared the 215 program to fire insurance. "I buy fire insurance ever since I retired, the wife and I bought a house out here and we buy fire insurance every year. Never had a fire. But I am not gonna quit buying my fire insurance, same kind of thing." (Lake 2014)

In both, the refrain that holds the logic together is simple: 'you never know'. Semantically, of course, 'you never know' means just that: *you will never know for sure* whether surveillance is necessary, whether we will regret our surrender of privacy, whether the terrorists would have 'got you'. Yet the attitude they incite is exactly the opposite: since you will never know, *you have to do something about it.* Love it or hate it, state surveillance in the post-Snowden era certainly requires your imagination – or, more precisely, your willingness to project your affects and your reason forward unto the uncertain future.

This chapter thus argues that the known and the unknown are not simple opposites laid out on an epistemic switchboard of 0s and 1s. Knowns are shaped out of unknowns (and continue to harbour uncertainties), while surveillance, as a technology of knowledge production, itself contributes to uncertainty. Snowden's sympathisers hailed the leaks as a paradigmatic instance of *transparency*: the belief in the public aggregation of solid, stable facts upon which deliberation might occur. Transparency quickly became the axiom by which Snowden could be justified (Fantz 2013) and the state could be lampooned (Kravets 2013; *The Washington Post* 2013) – at least, when the state wasn't itself admitting that the leaks indeed delivered "some needed

transparency" (Crawford 2015).[15] Transparency discourse projects a public that will readily take possession of offered information, and upon digesting it, come to a rational consensus (e.g. as critiqued in Dahlberg 2007). But the many ways in which surveillance is entangled with uncertainty is not reducible to explanations at the level of ignorance, obfuscation or even secrecy – although all of those things do feature prominently. It is also a matter of how aspects of the world out there (or, in Wittgensteinian terms, states of affairs) *appear* into our experience, manifest a presence, call for our attention – or withdraw from them (and, sometimes, loudly announce their withdrawal).

Such a story necessarily takes as protagonist not the secret reality or truth itself, but the objects that carry into the public the *relations* of exposure, of simulation, of uncertainty, of approximation. These I call *recessive objects:* objects whose appearance promises our access to objective reality, but in doing so, also serves to emphasise our removal from 'what is really going on'. Objects whose informational value is undeniable in terms of their content, but

[15] Another key group of actors were tech companies – some of which were revealed by Snowden to have passed personal data onto the NSA. After the initial, obligatory performance of shock and surprise, many companies took to championing transparency, issuing reports of government data requests with much fanfare and publishing open letters in the name of openness (e.g. Kopstein 2013; Hill 2013; Sanchez 2013).

which generate speculative activity far outstripping that content. Recessivity is not ultimately a question of the objective property of such objects, but their social life: how something like the Snowden files, or the genre of CCTV imagery (e.g. Gates 2013), presents certain things as 'known', signals others as unknown or even unknowable, and normalises certain networks of legitimation or standards of verification. Objects like the Snowden files, which we invest with a presentational power: that they reveal some aspect of truth, of reality. Objects like 'metadata', which take on a certain mystery, potentiality, and thereby become virtual objects in the Deleuzian sense. Some objects elicit perturbation, panic, indignation. Other objects become authoritative bastions of certainty, firm ground that we can base our opinions and sentiments on, objects that hold the real in place for us. So this is a story of how our investment in notions of objectivity, privacy, national security, involve taking pervasive existential and epistemological uncertainties and developing conventional ways of *translating* them into the sufficiently known, the 'real enough' (Hong 2015).

Recessive objects, therefore, describe things whose appearance into the public domain (and thereby lived experience, if only lived experience of the mass media) stand in for the non-appearance of others; objects which reveal certain

aspects to experience and withdraw in others; objects which provide material anchor for the collective efforts to establish 'known facts'. This chapter traces the public presentation of two different objects, tracing their network of references in the Snowden debate to identify their influence. The first is, of course, the Snowden files: an archive of unknown size whose content has exposed much about the NSA in a highly concrete fashion, and yet is also an object of speculation and mystery. The second is the lone wolf terrorist, the antagonist at the heart of the narrative of New Terrorism. The lone wolf is by definition unknowable, inexhaustible, uncontainable; a figuration of the irreducible uncertainty at the heart of surveillance. Both objects are figurative – a set of imagined properties and epistemic potential anchored onto a concrete object (which is now made a little larger than life). Each object makes a specific articulation of the problem of recessivity: what is the evidentiary function of proof that is technically available but so often, practically, goes unseen? What is the definitional and classificatory work performed by a label which ultimately points to the impossibility of knowing the threat?

In both cases, my focus is less on purposeful strategies of obfuscation and concealment, or the more absolute kinds of secret that are utterly hidden from public view – though those things, too, enter into the analysis, and work done

in this area are important precedents.[16] Rather, this chapter emphasises the ways in which the unknown is presented for the work of knowing, all the while retaining its unknowability. Through these objects, I ask: what are the social systems of knowing that rationalise and problematise contemporary online surveillance? How does the reason of surveillance promise to combat and destroy uncertainties, and at the same time relies on them to justify its existence?

THE SNOWDEN FILES

Let us return to where we started: the documents. The powerpoints, memos and reports were supposed to finally give us the unvarnished truth, a primary and original evidence. In a debate where critics of surveillance had perennially been marginalised as paranoid rabble-rousers, and tended to rely on anonymous whistleblowers and general descriptions, the files were credited as being the "first concrete piece of evidence exposing dragnet domestic surveillance" (Kelley 2013), the "first direct evidence of unlawful

[16] Such 'produced invisibility' would include the pre-Snowden status quo, where the intelligence agency and the executive branch had gone to great lengths to remove even recessive objects of surveillance from the public eye. Surveillance, despite a series of earlier leaks, remained a kind of unknown unknown, pursued by writers like James Bamford (2008). It would also include problems like the absence of data on 'police killings' in the United States, which consists a structural disruption of the work of knowing (Gates 2015). In such phenomena, it is more possible to delineate knowledge work proper from practices seeking to disrupt and destroy that work. Meanwhile, our analysis of recessivity and uncertainty addresses the speculative and uncertain lurking in precisely the work of knowing.

NSA spying" (Gallagher 2013). Indeed, previous NSA whistleblowers – William Binney, Thomas Drake, J. Kirk Wiebe – have pinpointed the files as "documentary evidence" and "material evidence" that finally grant additional weight to their own allegations (Eisler & Page 2013). CCTV images, we know, have long permeated the popular imagination of 'authentic' surveillance, to the point where video forensic workers add in once classic, now obsolete features like time-codes with the sole purpose of tapping into this latent legitimacy (Gates 2013). Similarly, the Snowden files are bestowed with a certain veridical authority. The documents were treated as producing a more raw and authentic kind of evidence: material, concrete, 'documentary'.

Indeed, the Files' contribution to 'on-hand' public knowledge is considerable, whichever way you cut those words. XKEYSCORE; Gilgamesh; Rhinehart; BOUNDLESS INFORMANT; PRISM; Project Chess… entire programs were dug up out of complete obscurity. Yet even as secret surveillance is brought into the domain of the knowable, this narrative of transparency and public knowledge is predicated on further emphasising the world of uncertainties and unknowns still to be unmasked. The files themselves not only encourage suspicion and speculation, but build up their veridical authority precisely through this encouragement. This section traces the files' public presentation

as evidentiary objects, and the recessive relations contained therein. It considers how the files present the idea of specific, transparent information, but appear just as often in the form of an uncountable multiplicity, a swarm. It describes how, rather than eliminating uncertainty about state secrecy, the files give material authorisation to further speculate about what remains unknown: paranoia and conspiracy is here a structural condition of the epistemological relation, rather than psychological ailments or 'feelings' per se. In considering the co-dependent, co-productive relationship between knowledge and uncertainty, my objective is not to argue that such leaks harm democratic deliberation, or that they are not informative. It is to understand how the mobilisation of such 'documentary' evidence entails a redirection and reorganisation of who/what knows *for* the public; what is designated as 'must be known' or 'cannot be known'; and what the public is told can or must be done with this new knowledge.

***

On 20 July, 2013, journalists at *The Guardian* descended into their basement, power drill and angle grinder in hand. Observed by two UK state officials, they proceeded to physically eliminate the offending laptop: the one which

contained secret NSA files leaked by Edward Snowden (Rusbridger 2013). It was, of course, a purely ceremonial gesture; Snowden's files had already been distributed to a global network of journalists and activists (Farivar 2013), including *The Guardian*'s own offices in the U.S. The drill-and-grinder ritual reflected not only the difficulty nation-states face in combating online information flows, but just how distributed and multiple the once-secret files had become. Smuggled out through mundane USB drives (Zetter 2013), the exact size, scope, and location of Snowden's digital trove captivated the attention of American news media (e.g. Cole & Windrem 2013; Hosenball 2013; Borland 2013; Goldman 2013; Almasy 2013). Not that anyone could figure out just how many documents even existed. This was, in fact, a hotly contested question, because Snowden himself never deigned to supply a number. Glenn Greenwald, Snowden's primary journalist contact, has refused to give a firm number; the closest he came was in an obscure New Zealand television appearance, where he referred to 'hundreds of thousands' of documents (*The Nation* 2014). Janine Gibson, the Editor-in-Chief of *The Guardian* US, claimed 'over 58,000 files', but apparently only once – at an event at Columbia University (Bell et al. 2014). In fact, the figure 58,000 only appeared in mainstream news outlets as part of the false rumour that David Miranda, Greenwald's partner, was detained in Heathrow with that number

of documents (Greenwald 2015). Meanwhile, the U.S. government also tossed numbers into the air. A Defense Intelligence Agency report to Congress about the leaks claimed that Snowden took 900,000 files from the Department of Defense alone – distinct from his haul from the NSA (Leopold 2015). One of the most widely cited estimates was that Snowden "touched" – that is, accessed – 1.7 million files while contracted for NSA work at Hawaii (Kelley 2014). This figure has sometimes been misconstrued – by media as well as U.S. Senators[17] – as documents *taken* by Snowden, a conflation about which Glenn Greenwald has publicly expressed frustration (Greenwald 2015). At the end of the day, the quantity of documents remained a secret, even as estimates came and went with a margin of millions.

It is ironic that the NSA should be more forthcoming than its critics about the quantity of documents. The months it took them to come up with even approximate figures, and the reluctance to advertise them prominently, suggests that the government itself does not know for sure. Indeed, this prevarication itself was criticised: why should we trust the government to keep our secrets secure, when they can't even figure out what the thief has

[17] Senator Susan Collins raised the figure in the 2014 hearing for the Select Committee on Intelligence of the U.S. Senate, which is officially open to the public (*U.S. Senate Select Committee on Intelligence*).

stolen? (Friedersdorf 2015) In fact, US state surveillance has already had this problem for years before Snowden. The development of the vast electronic dragnets Snowden has exposed required a massive boost in the NSA's funding, and a corresponding boom in internal hires, new infrastructure, and outsourcing contracts to the private, military-industrial arm of the surveillance apparatus (e.g. Shorrock 2015). The consequence was that by 2010, it lacked comprehensive and precise metrics for mapping its own surveillance apparatuses, or estimating the overall costs of anti-terrorism (Pasquale 2015, p13; Bamford 2008, p199). As if a parody of banks 'too big to fail', the landscape became littered with big data that is too big to account for.

This question of numbers is not trivial. The quantity of the documents here becomes a proxy for asking: what is the information that we now 'have' but still cannot access? What remains secret about that which is technically exposed, and what wider landscape of secrets does such exposure gesture towards, emphasise, visibilise? Peter Galison (2008) reports that the U.S. government as a whole has 'reportedly' classified 92,064,862 documents in the single year of 2011. Not even 1.7 million scrapes the top of the iceberg. From a different angle, the secrecy archive Cryptome (2016) provides us with an entertaining estimation. In October 2013, it wrote: "out of reported 15,000

pages, The Guardian has published 192 pages in fourteen releases over four months, an average of 48 pages per month, or 1.28% of the total. At this rate it will take 26 years for full release." Two years later, estimates had grown less, not more, precise: "20-620 years". As is so often the case, the joke is the vehicle for the serious. We are faced with either learning more about the NSA until the day we die, or getting so much information so fast that we can never expect to read most of it – the latter route exemplified by earlier leaks from Julian Assange's WikiLeaks.[18] The widespread speculation over the number of documents illustrates how, distinct from a select few documents grasped in their specificity, the public impact of these evidentiary objects must be understood in their appearance as a multiplicity, a swarm. What becomes a public object of concern is the forest as much as the individual trees.

The problem of large numbers was not just a problem of scale, of having too many documents for one individual to process, publish or read. As with the advent of statistical law and normal distribution models over the 18th and 19th

[18] In fact, WikiLeaks' files had their own correlate of the numbers problem: the 'insurance file'. In July 2010, the group uploaded a 1.40gb file named 'insurance.aes256' – the file extension revealing its use of the relatively highly secure (though of course not uncrackable) AES256 encryption. It has been variously reported as 'insurance' or Julian Assange's 'poison pill', a file which is presumed to contain as-yet unknown government secrets that would be revealed should Assange come to harm. Subsequent insurance releases grew in size, reaching a gargantuan 349 gigabytes in 2013. Again, the numbers provide not specificity, but an open space that attracts speculation.

centuries (spurred in part by massive growths in urban populations) (Hacking 1990), or the new hopes for total collection and analysis provoked by the emergence of 'big data' in the early 21st century (boyd & Crawford 2012), the problematisation of large numbers entailed qualitative shifts in the *how* of knowing. In the case of the Snowden files, these numbers indicate and visibilise a space for speculation and estimation distinct from the documents' promotion as concrete and documentary. We find an extreme illustration of this predicament in Borges' *The Library of Babel.* "When it was announced that the Library contained all books, the first reaction was unbounded joy" – and soon after, "a similarly disproportionate depression." (1998, p115-6) Though the denizens knew in theory that the Library *actually* contained every combination of letters and words, their experiential access to this world was only achieved through the idea that every book is *potentially* readable and findable out there. Hence "in order for a book to exist, it is sufficient that it be *possible.* Only the impossible is excluded" (ibid., p117). We must recall that the sheer size of the Snowden files is not only a comment on the whistleblower's methodical process, but the complexity of the secret surveillance apparatus itself. The fascination with the number of documents contributes to and springs from the wider attention upon the wilderness of the unknown, a surveillance system that one can never claim to 'know' in full. In short, the

numbers – as one artefact of the Snowden files as a whole – present a recessive relation, wherein the presentation of vast quantities of evidence serves to emphasise the unknowns that now attract renewed attention and speculation.

Meanwhile, the size of the documents created another problem for information and transparency: who has even read all the *published* documents? What does a revelation prove if nobody's peering in through the unlocked vault – not even Edward Snowden himself? In a 2015 interview, Snowden was unable to confirm if even he himself had read all the documents, and was forced to dodge the question multiple times (*Last Week Tonight with John Oliver* 2015). This half-admission was widely reported by Western news media as probable proof that he had not (e.g. Akkoc 2015; Kelley 2015; *One News* 2015). Not even Edward Snowden could give the public certainty that, if not they themselves, *somebody* has read and checked the proof. As for the lay public, Snowden's decision to leak the documents in a gradual, journalist-mediated flow did not make life any easier. Table 1 is a non-complete listing of reportage based on the Snowden files from the initial leaks in June 2013 to the end of the calendar year, containing only what I considered sufficiently distinct pieces of news. Meanwhile, Table 2 lists

original Snowden documents released through *The Guardian* in those first few months – leaving out files handled by other publications and organisations. How many Americans could reasonably be expected to read every published document – or to maintain an accurate picture of what has been proven and what remains speculation? A survey, addressing news habits in the first four days of the Snowden leaks (6-9 June 2013), suggested that 50% of the Americans followed the news 'not too closely' or 'not at all closely' (Pew Research Center 2013); we might well expect public attention to have declined in the ensuing weeks and months. The public is, ever so often, a device by which the few can make claims about and on behalf of many. But the Snowden files point to an enduring ambiguity between public and publicity. Not only are large parts of this amorphous public unlikely to have first-hand knowledge of the evidence, but coupled with their *awareness* of the evidence's availability, the leaks can generate rather than quell speculation.

13.12.13	NSA cracks cell phone encryption for A5/1 (2G standard)
13.12.10	NSA uses cookies to spy
13.12.09	NSA uses video games to spy
13.12.04	NSA collects 5 billion phone records per day
13.11.26	NSA spies on pornography consumption habits
13.11.23	NSA 'Computer Network Exploitation' infects 50k networks
13.11.14	CIA collects bulk international money transfers
13.10.31	NSA hid spy equipment at embassies & consulates
13.10.30	NSA attacks Google & Yahoo data centres
13.10.24	NSA tapped 35 world leader calls
13.10.21	NSA spied on Mexico's then-president Felipe Calderón
13.10.14	NSA collects US address books, buddy lists
13.10.04	NSA can hack Tor
13.10.02	NSA stores cell phone locations up to 2 years
13.09.30	NSA stores metadata up to a year
13.09.28	NSA maps Americans' social contacts
13.09.16	NSA 'Follow the Money' division tracks credit card transactions
13.09.07	NSA can tap into smartphone data
13.09.05	NSA attacks encryption standards and hacks
13.08.29	US intelligence 'black budget' discussed
13.08.23	NSA employees spy on ex-lovers
13.08.15	NSA internal audit shows thousands of violations
13.07.11	XKEYSCORE revealed
13.07.10	NSA 'Upstream' fibreoptic spying capacities revealed
13.06.30	Additional PRISM leaks
13.06.19	NSA 'Project Chess' for Skype revealed
13.06.17	Apple, Microsoft, Facebook release collection procedure details
13.06.16	NSA spied on Dmitry Medvedev, then Prime Minister of Russia, at the 2009 G20 summit
13.06.11	BOUNDLESS INFORMANT revealed
13.06.10	Edward Snowden named
13.06.09	NSA record/analysis tools leaked
13.06.07	'Presidential Policy Directive 20' revealed
13.06.06	First leak: PRISM program revealed

Table 1. Snowden's revelations, June-December 2013.

Number	Date	Title	Pages
	The Guardian		**276**
	27 February 2014	GCHQ Optic Nerve	3
21	16 January 2014	SMS Text Messages Exploit	8
20	9 December 2013	Spying on Games	2
18	18 November 2013	DSD-3G	6
19	1 November 2013	PRISM. SSO SSO1 Slide SSO2 Slide	13*
18	4 October 2013	Types of IAT Tor	9
17	4 October 2013	Egotistical Giraffe	20*
16	4 October 2013	Tor Stinks	23
15	11 September 2013	NSA-Israel Spy	5
14	5 September 2013	BULLRUN	6*
13	5 September 2013	SIGINT Enabling	3*
12	5 September 2013	NSA classification guide	3
11	31 July 2013	XKeyscore	32
10	27 June 2013	DoJ Memo on NSA	16
9	27 June 2013	Stellar Wind	51
8	21 June 2013	FISA Certification	25
7	20 June 2013	Minimization Exhibit A	9
6	20 June 2013	Minimization Exhibit B	9
5	16 June 2013	GCHQ G-20 Spying	4
4	8 June 2013	Boundless Informant FAQ	3
3	8 June 2013	Boundless Informant Slides	4
2	7 June 2013	PPD-20	18
1	5 June 2013	Verizon	4

Table 2. Cryptome's tally.

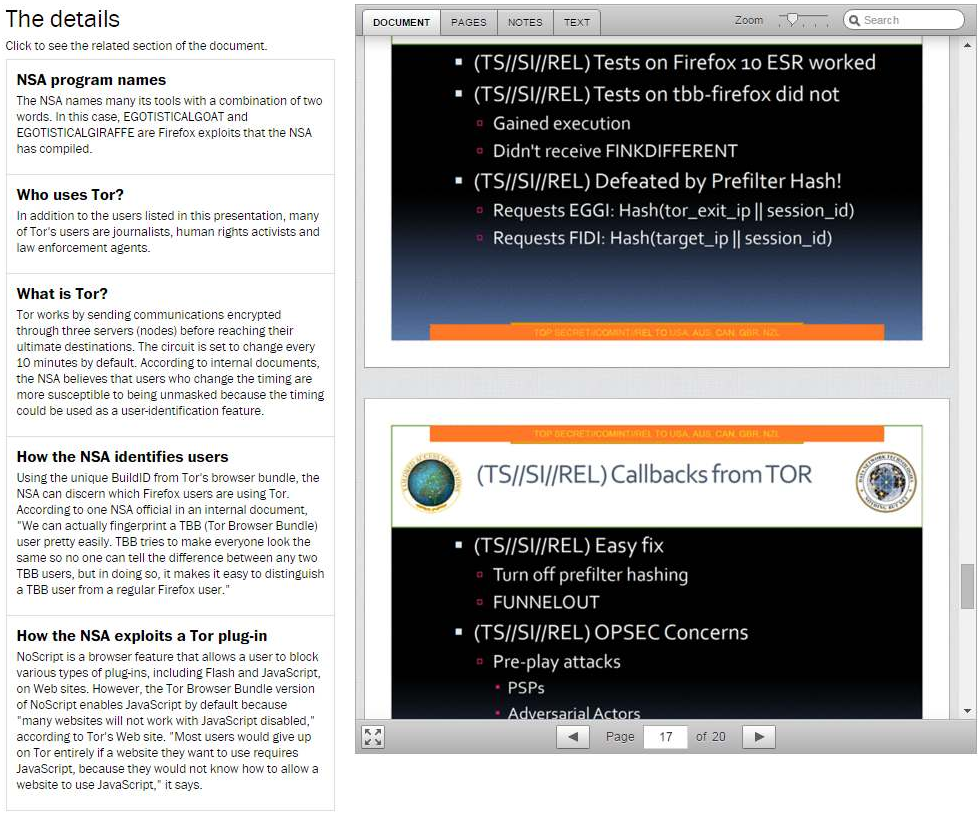


Figure 1. A typical Snowden file.

Where the documents themselves *were* directly consulted, they often proved jargon-laden and requiring a great deal of technical and institutional context to parse. The Snowden files, after all, were primarily PowerPoint presentations, internal memos and instructions, designed to brief NSA employees about what their own organisation was doing (or wanted to present themselves as doing). For instance, public reports on the NSA's technologies for collecting and analysing online oral communication were sourced from short written brief by the NSA for the NSA, promoting its own software to analysts that might have overlooked them (Froomkin 2015). The

reportage thus depended on the interpretive labour of journalists like Glenn Greenwald and Barton Gellman to guide the user through terms like "selectors detasked", or codenames like Pinwale and Egotistical Giraffe (Gellman & DeLong 2013a; Rich & DeLong 2013; also see Fig.1). And each one, of course, opens its own set of rabbit holes: an intrepid reader might find themselves reaching back to pre-9/11 programs like Echelon and Stellar Wind, scrolling through reams of legalese that try to explain why metadata collection is sufficiently like retrieving call records from landline providers and not sufficiently like warrantless wiretapping, and so on. Even when the technical details are not overwhelmingly difficult (or just wearisome), every new revelation reignites conflicting speculations about what these programs *could* do and what they end up meaning in combination. When the concerned citizen learns that the NSA collects millions of texts, but they can vaguely recall that they also collect millions (or was it billions? Trillions?) of phone records and international money transfers and social media photographs and email address books, but it's not necessarily any and every text or phone call, and then there are minimisation procedures, and … And yet, the documents, and what they are able to authorise as facts, exert a palpable presence upon the public imagination of surveillance. Evidence does not extinguish uncertainty, but redirects it and refocuses it. It is only because the documents

exist that the subject can enter into speculation, indignation, scepticism – even if they may not be quite sure what is and isn't in those documents.

***

None of this takes away from the documents' public status as powerful evidentiary objects. State surveillance had for decades operated as *public secrets*: that which is generally known, but cannot be publicly articulated (Taussig 1999). With the Snowden files, the veridical authority endowed them now pushed the threshold of plausible deniability by an appreciable amount. Yet at the same time, the documents' presence as proof, as swarm, as number, as indicators of further secrets and potential harm, served to open up new spaces for *paranoia*. I do not mean that millions of individuals will specifically feel that the government is out to get them. Rather than the content of subjective experience, I am describing the structure of an epistemological problem that the Snowden files publicises. The files' appearance as veridical objects provoke a renewed focus on surveillance's secrets; the public is thus presented with an urgent necessity for constructing meaning – even when, especially when, there are clear unknowns. The paranoid epistemology exhibited in the Snowden Affair may thus be considered an extension of what

Richard Hofstadter (1967) called the 'paranoid style' in American politics: a tradition of conspiratorial and indignant mode of expression that can be identified in McCarthyist America of the 1950s, and even to the moral panic over the Illuminati in the late 18th century.[19] I also turn to Carl Freedman (1984), who describes Freud's paranoia as a "ruthlessly hermeneutic logic" that takes more normative styles of reasoning and amplifies their tendency to systematically fit everything into an intelligible pattern. In applying paranoia to science fiction, his analysis also demonstrates the epistemological, rather than psychopathological, conceptualisations of paranoia: a relentlessly consistent and systematic grid of intelligibility used to answer every kind of unknown.

There is an apocryphal story that some conspiracy theorists were rather put out when the Snowden leaks happened: now their theories had been proven right, they'd have to come up with some new ones! Being proven right is not the end of paranoia. For a more concrete example, consider a post on reddit's /r/conspiracy, a hangout for conspiracy peddlers (or, as the site itself puts it,

[19] One notable difference: while Hofstadter too refrains from the clinical meaning of paranoid as a sickness, he is unapologetic about describing the paranoid style as making a "curious leap in imagination" that ultimately departs from the world of actual facts (1967, p37-8). Here, I make no such assumptions about the 'actual' accuracy of paranoid claims; how could I, or anyone else, do so when the structure of secrecy and uncertainty ensures the public shall never know for sure one way or another?

'free thinkers'): "If it weren't for Edward Snowden conspiracy theories would still just be 'theories' … High five to the sane ones <3" (*Reddit* 2015). Yet even this is naïve, since paranoia will always point towards a greater secret behind appearances: "So you're thanking a guy who at least previously worked for the CIA (and most likely still does) for making *conspiracy theories* validated, when it was the CIA who literally weaponised the term *conspiracy theory* as a PR campaign to cover up for the Warren Commission?" Paranoia was presented as an *appropriate* technique for intelligibility in mainstream news media as well. Conspiratorial language was commonplace, especially amongst those critical of Edward Snowden. Speculations that he was a Russian or Chinese double agent, or at least their gullible puppet, were fuelled by Keith Alexander and other high-ranking NSA officials (e.g. Cohen 2014; Kaczynski 2014; Johnson 2014; *Fox News* 2013). One *Washington Post* piece suggested that Glenn Greenwald, Julian Assange and others had conned Snowden into risking his life for the former's ambitions – at least, before the paper issued a series of corrections (Pincus 2013). Of course, there were also public statements seeking to quell paranoid reasoning, arguing that the terrorists are hoping to induce paranoia and the risk posed by terrorist attacks is in fact rather small (e.g. Krauss 2016). But whereas such cautions relied on a binary of reason and paranoia, what is most striking is the degree to which

paranoia can be *reasonable* to the information environments people find themselves in. The Affair exhibits not a new low in irrationality amongst the population, but how the deployment of 'collect 'em all' surveillance strategies and 'reveal 'em all' whistleblowing responses served to legitimate paranoid heuristics as practical epistemologies.

Thus, the Snowden files become generative of new theories, new speculations, projecting ever larger shadows behind what it reveals. Indeed, one pro-surveillance article made the case rather bluntly: "fearing the NSA… requires you to believe that hundreds, if not thousands, of American employees in the organisation are in on a conspiracy." (Gerecht 2013) The only *reasonable* solution, they go on to conclude, is to trust in the NSA, since not trusting would require us to be, well, paranoid. What matters is not the information these documents provide, but a variant of what Tor Nørretranders (1998) calls *exformation*: the inverse of information, the bits that are 'explicitly and knowingly discarded'. The bits that the available information leaves unsaid and unproven, but now gain a social presence in a provisional and anticipatory form. A paranoid epistemology is thus an apophenic one: the trouble is not that meaning is *secret, hidden, lost,* but that it is *too much and everywhere* (Steyerl 2016). This paranoid mode of sense-making is replicated

on the side of surveillance's critics. Suspicion of Snowden's motives were frequently met by the thought that the leaks were in fact engineered by the U.S. government. This was a classic case of what has since Watergate been called 'limited hangout': a deliberate admission (or even revelation) of certain embarrassing details in order to conceal even worse ones. The *importance* of the unknown, the unknown as must-become-known, is thus emphasised precisely through the presentation of knowns. Walter Benjamin wrote that "truth is not a process of exposure which destroys the secret, but a revelation which does justice to it" (2009, p25). Secrecy is indeed not destroyed by the leaks, but endowed with a new kind of presence.

Paranoia, in this epistemological sense, reflects shifts in how knowns and unknowns become demarcated – not only in the fluid and relatively informal space of public deliberation, but institutionalised stages like the courts. Snowden's first leaks in 2013, and their most direct predecessors by *The New York Times* and *USA Today* in 2005-6, spurred a series of legal cases where plaintiffs, typically organised by civil rights groups like the American Civil Liberties Union [ACLU] and the Electronic Frontier Foundation [EFF], sought to bring state surveillance activities under public judicial scrutiny. In each of these legal contests, the most important issue turned out to be a basic question

of available facts: what kind of harm is *known* to be caused by surveillance? Despite the new availability of Snowden's files, efforts to contest NSA surveillance at the judicial level struggled to gain standing due to the difficulty in constructing a definition of surveillance harm that is compatible with the existing legal conceptualisation (in the United States) of harm as 'concrete, particularised and actual'.[20] In *ACLU v. NSA* (2007), the District Court concurred that phone/internet data collection is not only unconstitutional, but *does* count as concrete, particularised and factual harm; however, the 6th Circuit Court of Appeals ruled that the injury claimed is 'mere belief' of intercepted communications, and the lack of any 'personal' harm, only a 'possibility', denied them standing.[21] For that matter, what harm is known to be *prevented* by surveillance? Despite its voracious ingestion of data over the last decade, the NSA, too, have found it difficult to produce concrete proof that surveillance has stopped terrorist attacks. Having initially cited '54 plots' foiled by metadata collection, NSA spokespersons were soon forced to admit that there was really only one case that could be presented

[20] This definition is part of a stable chain of precedents established by Supreme Court decisions, including *Lujan v. Defenders of Wildlife* (1992), *Warth v. Seldin* (1975) and *Sierra Club v. Morton* (1972). For instance, *Jewel v. National Security Agency* (2011), filed by the Electronic Frontier Foundation on the basis of earlier leaks by Mark Klein, was judged upon these terms, and ultimately granted standing upon appeal.

[21] Similarly, in *ACLU v. Clapper* (2015), the U.S. government sought to have the case thrown out on precisely this lack of standing, and nearly succeeded; the case is still in process at time of writing.

with certainty (Schwartz 2015).[22] Such debates reflect a fundamental problem with public secrets: what must one 'know' in order to bring the unknown into trial? What should and should not count as 'known' in the face of such relentless uncertainty?

The potential and futuristic designation of harm – from both sides of the debate – exemplifies the way in which recessive objects fuel, not replace, the work of speculation. Its defenders and critics fight to prove the reality of a future which it is their mission to prevent from actualising, and this necessitates both sides to engage in an array of what-ifs and you-never-knows (a problem that we shall return to in Chapter 3). Yet to label such strategies irrational, and deplore them as a collective turn towards epistemological parlour tricks, would be to reproduce the ideal notion that information should lead us to proof and certainty. Rather, paranoia serves as an epistemological technique for integrating unknowns into reliable frameworks for understanding – a technique which is presented as contextually appropriate

[22] This was the arrest of Basaaly Moalin in 2010, whose phone metadata showed him in contact with an Al-Qaeda member. While other cases have been connected to NSA surveillance, Susan Landau (2013) has convincingly debunked the idea that PRISM-style dragnets played a critical role in them; and a White House review of the NSA surveillance program wrote that "there has been no instance in which NSA could say with confidence that the outcome would have been different without the section 215 telephony meta-data program" (Clarke et al. 2013, p120).

and *normal*. It is a historical extension of what Tobin Siebers (1993) called the 'cold war effect': a generalised epistemological climate where paranoia and suspicion were seen not as delusions or pathologies, but virtues, and to be paranoid was not to be ill but to be in tune with contemporary reality. (Indeed, there are literary and political connections between certain cold war tropes and Snowden-era paranoia (Melley 2012).) Merleau-Ponty (2012) understood this when he noted that for subjects of madness, their madness is not error or illusion, but a naturalised and intuitive access to truth. A schizophreniac experiences voices not as hallucinations superimposed over reality, but something as genuine as the ground beneath our feet. (Merleau-Ponty thus describes a schizophrenic woman who believes two individuals with similar looking faces *must* know each other: a connection which 'normal' humans would dismiss as apophenia gone haywire, but for the woman is simply common sense.) The point is that any given system for rendering the world around us into intelligible pieces requires some reliance on presumptions about the unknown – a reliance which, to outsiders, appears arbitrary or nonsensical.

Such reliance is necessary because not only can we never know everything in a general sense, but we often do not know what our epistemological

framework *defines* as important and necessary information. So it is the case with the problem of harms, and – as we described earlier in this chapter – the refrain that 'you never know'. To be able to exclaim that 'you never know, but (so) we have to do something' is to be *paranoid enough* to see past the unknowns and connect the dots yourself. It may be technically prudent to wait until all the facts are in hand, but in the case of a secretive surveillance program and the logic of preventive prediction, nobody will ever reach such a privileged position. The Snowden files pair certainty with speculation precisely by forcing the unknown out of negligibility and into the status of active problem. They assert the collective need to render this entanglement of knowns and unknowns into a meaningful, actionable narrative.

This entanglement of information and uncertainty, emblematised by recessive objects like the Snowden files, makes a parody of the current enthusiasm for transparency.[23] Transparency is axiomatic for whistleblowers, of course, and Snowden himself framed his actions in this light (Fantz 2013), but liberal democratic governments have also embraced it in their rhetoric (if not always their practice). Buzzwords bloomed by the dozen in the wake of enthusiasm

[23] Some of the following analysis on digital transparency have been adapted from another piece (Hong & Allard-Huver, Forthcoming).

about 'ICTs': e-government, e-transparency, e-democracy… In this idealised form, transparency frequently communicates a belief in the 'virtuous chain' of information, rational deliberation, and democratic participation – all of it jumpstarted by new media technologies.[24] But, as we have seen, there is no easy connection between the theoretical availability of information and its uptake as knowledge (also see Vattimo 1992). Even widely reported information provokes mediated speculations and sentiments, not to mention felt uncertainties. In the Shannon-Weaver model of communication (Shannon & Weaver 1963), information is essentially defined as the reduction of uncertainty. This definition, of course, was never intended to encompass every definition of information, let alone knowledge. The point is in the contrast: with cases like the Snowden files, we find that the presentation of solid, reliable information can *increase* the public labour of speculation and inquiry.

Alongside the gloss of 'power to the people', the less attractive side of the transparency bargain is that it levies labour and responsibility upon the citizen. Transparency can thus be a barrier to becoming-political. In the

[24] As one prominent example, we might consider one of Barack Obama's first communications as the President of the United States: a memorandum titled 'Transparency and Open Government' (Obama 2009). Its easy equation of transparency with accountability and informed citizenry exemplifies the period's enthusiasm for the idea.

context of liberal, representative democratic societies, transparency mobilises the citizen anew with an old responsibility: not just to participate in politics in prescribed moments and ways (e.g. voting every four years), but to become an unblinking eye poring over every aspect of government. The citizen has been recruited as a free auditor for the state. This is to be distinguished from earlier forms of citizen redress, such as petitions of grievances and injustices. The long Western history of petitions, from written pleas to the Roman Emperor to the cahiers de doléances in 1789 France, were not the normal duty of subjects, but extraordinary actions – while the work of assessment and redress remained the task of the governing Prince (also see Zaret 2000, p59). This was also the case for the literary trope of the King who speaks with his subjects in disguise to hear their grievances – most famously Shakespeare's Henry V, and James V of Scotland's legend as 'King of the Commons'.[25] Again, it remained the King who must listen, to gather data, to make his population legible, and to reconfigure his apparatuses of government according to that knowledge. In the e-transparency paradigm, the government (or the whistleblower) uploads, makes 'available' – a passive

[25] Stories of James V's disguised outings, recurring in various forms ever since the years of his reign, were themselves part of a wider folklore motif of the king-in-disguise. The accuracy of such stories as pertaining to a specific monarch are generally unverifiable, but they as a whole gestured to a popular belief that positioned the King as monitoring (benevolently) his subjects (e.g. see Stevenson 2004, p198).

position, after which it is the public's responsibility to request, read, cross-reference, judge, prosecute. The proof may be *in* the Snowden files, but the burden of proof is *on* the subject.

The problem is that much of the time, it is a burden that subjects cannot afford to or are reluctant to bear (see Bannister & Connolly 2011). When another realm of online surveillance – corporate data-mining – became scrutinised for invasions of privacy, one popular solution was to push for greater transparency on the part of online platforms. Predictably, the result was an even greater onslaught of privacy policies that many people do not want to read, do not have the time to read, and do not have the background knowledge to fully understand. As one study showed, it would cost $781 billion per annum in salary if Americans used their working hours to read the privacy policy of every site they visited (McDonald & Cranor 2008). In any case, scrutiny enabled by such 'transparency' is as often a melange of misunderstanding, confusion and second-hand interpretation, as evinced by numerous incidents where even efforts at clear and accessible policies have resulted in speculation and panic.[26] The impossibility of fully taking up, or

[26] One example is that of Snapchat, a social media platform where users send text/image messages that automatically expire after ten seconds. In 2015, news media reported on new privacy policies, warning for example that Snapchat "now owns the rights to all your nude photos forever" (Russon 2015). The irony is that Snapchat (2015) claims it only ever updated

'owning', the burden of transparency produces a new chain of deferrals and delegations. An act of transparency, like Snowden's leaks, often yields secrets revealed but unread, and identifies new secrets now to be speculated over. The idea that the good citizen ought to now know for themselves can also produce a space, a gap, which is then filled by deferred and presumed forms of knowing.

This is not a critique of transparency not being 'good enough'. That would imply we need to try and make sure transparency 'properly' informs citizens and enable sovereign judgment and agentic action. The point is that 'to know' is a complex, mediated, and costly business, such that the injunction to know generates new techniques and habits by which we can *avoid* the work of knowing for ourselves. Slavoj Žižek asks: why do we only focus on the restrictive or oppressive dimension of Foucaultian discipline? Discipline is also a kind of liberation:

> This liberating potential of mechanical rituals is also clearly discernible in our modern experience: every intellectual knows of the redeeming value of being temporarily subjected to the military drill, to the

---

the policy "so that they'd read the way people actually talk." This apparent attempt at transparency ultimately required Snapchat's own clarifications (ibid.), and news articles translating those clarifications back into 'what's really going on' (Howard 2015) – all in addition to the original 2660-word privacy policy and 4102-word terms of service.

> requirements of a 'primitive' physical job, or to some similar externally regulated labour — the very awareness that the Other regulates the process in which I participate, sets my mind free to roam, since I know I am not involved. The Foucauldian motif of the interconnection between discipline and subjective freedom thus appears in a different light: by submitting myself to some disciplinatory machine, I, as it were, transfer to the Other the responsibility to maintain the smooth run of things, and thus gain the precious space in which to exercise my freedom… (Žižek n.d.)

In surrendering autonomy for parts of my own body and action, I become 'free' to pursue that which really matters to me. This, of course, is not so much a derivation of Foucaultian theory, but a faithful exegesis; from the Enlightenment project of discipline through (docile) bodies (Foucault 1995), to the voluntary optimisation of oneself by the neoliberal *homo œconomicus* (2008), and even the grand ordering and classifying devices of modern *epistemes* (2002), the bargain inherent in each regime of knowledge is that processes of ordering, determining, narrowing, are what enable the subject to exist and roam in a stable and recognisable system of meaning. Specifically in terms of bodily discipline, this is a principle that is more familiar to us as applied unto other peoples and machines (slaves, servants, secretaries, the role of women over the centuries). Žižek's example of the thinker also shows that this is not reducible to a clean *division* between the 'menial' aspects of my life and the important ones. The 'mindless work' of a military drill actively organises and direct the 'free activity' as well. The act of delegation does not

cleanly remove the subject from what the Other does for it, because this relation itself yields its own experience, and corresponding responsibilities, for the subject. In the face of so many uncertainties, and techniques of proof that seem to build upon rather than extinguish them, one can hardly insist that the individual subject 'know' all the facts and exercise their reason. What matters is the constellation of people, things and processes that 'know' on my behalf, and what kinds of responsibilities, decisions and rights that effectively leaves for me.

***

In Agatha Christie novels, we find the trope of the singular moment of revelation: when enough secrets (that is, *objective facts*) have been accumulated, the illusions topple all at once to reveal a perfect picture of the crime. The pleasure of this revelation is itself an expression of our shared intuition that, back in real life, things rarely seem to work out so neatly. Sherlock Holmes, too, insisted on a progressive and ultimately conclusive process: "when you have eliminated the impossible whatever remains, *however improbable*, must be the truth" (Doyle 2005, p36). Such a formulation is, of course, open to debate at metaphysical and meta-epistemological levels.

But we need not go that far. Holmes' world is an extremely finite and localised one: it is rare that the suspects and other characters do not wear every relevant aspect of their psychology and history on their person. But what happens when tens of thousands of government-employed analysts roam the four corners of the Internet, and reside in a complex the size of a small city (the NSA's Fort Meade is larger than Cambridge, Massachusetts in land area), when the nature of data collection mechanisms is such that nobody, not even the collectors, know whether your data will ever be seen by a human, when the very revelation of the secret involves an unknown (but vast) number of documents? Such linear eradication of the secret is replaced by an open struggle of speculative hypotheses that must all admit their partiality and uncertainty – even as they bid publicly for our belief.

This entanglement of knowledge and uncertainty comes down to a *gap* between the document as evidentiary object and the 'knowing' it is meant to produce: a gap which defies the transmissional imagination that proving, verifying and informing humans can work like a Windows file transfer. This gap is primarily at the level of neither metaphysics nor the content of individual experience, but the embodied and social structures that any 'knowing' depends upon. Known and unknown, transparency and secret,

turn out very rarely to manifest in such pure forms. The Snowden files, celebrated and feared in equal measure as 'exposure', were supposed to be as material and primary a proof as it gets, short of catching an NSA agent nibbling at your Ethernet cable. They were supposed to finally dispel uncertainty, and lay everything out on the table. But as we have seen, the documents' public presence is often in the form of a proliferation 'out there', rather than as specific and immediately available objects; the information gained from them act not to eliminate uncertainty, but to authorise new regions for speculative ventures. What does it mean for an object to acquire the status of proof? What other proof must exist for this object to function as proof, and what are the subterranean beliefs, objects, conventions, rhetorics, that prop up its veridical authority? Here we start to see the paradoxical wiring of knowing and uncertainty, of revelation and secrecy: it is the *recessivity* of data and technology, so fundamental to surveillance's project of knowing, that undergirds these phenomena.

RECESSIVE OBJECTS

The Snowden files' social function is both to cross the gap and to render it newly visible. This doubling is what I describe as recessivity. Recessive objects are objects whose social meaning and function are predominantly to

announce the absence of something *by making itself present.* Its own appearance reminds and visibilises the non-/dis-appearance of that referent. Sometimes, as with the Snowden files, the recessive objects themselves are seen to prove, clarify, enlighten; but in doing so, they also call attention to the sheer uncertainty of surveillance. Sometimes, the object itself is considered mysterious, insofar as it 'stands in' as a visible substitute for the invisible; this, we will see, is the case of the lone wolf. Where certain objects might be designed to conceal and erase the epistemic structure's dependency on uncertainty (such as the many conventions science has developed to present its objectivity), these objects' ability to *extend* our knowing to new regions come hand in hand with a visibilising of the reminder that we cannot, in some ways, know it at all. Recessivity, at the most generic level, is a paradox native to all methods of knowing, and particularly permeates our relationship to technology of every kind. This section thus draws on phenomenology, both 'classical' and contemporary, to more precisely define recessivity. It then describes recessivity as specifically manifest vis-à-vis the Snowden Affair. Knowing may always be deferred and simulated in some way, and every extension of our knowing may open up such 'gaps', but what matters is how different actors and values are arranged into what positions of power and

authority in a given context. Recessive objects illustrate and themselves help organise these relationships in that regime of knowledge/truth.

What exactly do we mean when we say objects make things other than themselves 'appear' – especially if that appearance is joined by a gap, a withdrawal? Phenomenology's basic conceptual vocabulary of presence and appearance allows us to sharpen the language of 'gaps'. In the original, Husserlian sense, *presence* denotes the fundamental relation of for-us that phenomenology investigates; it is the basic quality necessary for anything to exist for the human sensorium. But such an ontologically low-level distinction cannot easily handle the many ways in the human individual is mediated, distracted, technologised. Where Merleau-Ponty (2012) emphasised an integral I whose conscious experience folds different processes into a Whole, our concern here is a distributed kind of phenomenology, where we actively feel that what we know, what we see, what we feel, is not quite 'our own' (Rotman 2008; Thrift 2011).[27] Recessivity, after all, concerns not so much the

[27] This is not the place for a lengthy discussion of classical phenomenology, but my point is that its central concern with human access to the world around them involved this double-bind of extension and withdrawal. Heidegger (1962, I.3) famously wrote of ready-to-hand [*Zuhandenheit*] and present-at-hand [*Vorhandenheit*], describing the withdrawal of the object's thingness *relative to* human experience. The problem of *access* itself has been central to the entire project of phenomenology; from Husserl to Merleau-Ponty, to be human is to perceive the world by virtue of what we cannot perceive ourselves. In Graham Harman's latter-day revival, objects are considered *absolutely* withdrawn – an ontology where the gap is, for humans, fundamentally unable to be closed (2002).

aspects of sensory experience that are completely naturalised, but the ways in which the processes of knowing are openly problematised. In this sense, we might borrow from phenomenologists who have spoken of 'absent presence', and other hybrid complications of Husserlian presence. Here, 'absence' is not simply the inverse or lack of presence; the absence itself can be noticed, perceived, made into a collective object of concern (Frers 2013; Saury 2008). When the Snowden files point towards the deep secrecy of the state surveillance apparatus, the latter becomes caught in a position that is neither simple presence nor absence. On one hand, the files become stand-ins for the absent truth, bringing it out of the forgotten category of 'unknown unknowns'; on the other hand, the files cannot bring the secrets entirely to light, and serve to constantly remind us of that absence. To speak of absence, or non/dis-appearance, the unknown, the uncertain, is not to speak of being entirely cut off from them (an ignorance), but to describe how the problem of knowing is laid out for the public: what they must know, what is not possible to be known, what dependencies and presumptions are necessary for knowing, and so on.). In speaking of recessivity, we are pivoting towards the specific and structural relationships produced by the socio-historical definitions of knowledge and truth.

If the visibilising of uncertainty involves an 'absent presence', the other half of recessivity involves a kind of extension. As Žižek put it before, recessive objects are what we use to stretch our thinking, believing, opinionating far beyond our body, our experience, our ego. And that extension is precisely what creates gaps. Although objects like the Snowden files visibilise absence, secrecy, the unknown, they can hardly be said to have paralysed the public, or rendered them ignorant. This is not to simply say the human, who 'knows' the world, now knows quantitatively 'more', as if a hard drive that copied in more bits of data. It's about how the very way we think we 'know' things, and what kind of experience 'knowing' feels like, gets stretched, distributed, rewired. Recessive objects depict a landscape of mediating objects, always both material and semiotic, whose ability to associate invocations, ability to provide a sense of presence, ability to visibilise that which is beyond itself, allows us to reach out into the uncertain and the unknown in these variegated ways. Recessive objects thus constitute one generic mechanism for interweaving feelings of knowing and uncertainty.

Extended and distributed subjectivity has been a central trope in recent conceptualisations of new media. The proliferation of new technologies for knowledge production and sensory access has given rise to a range of

posthumanist ideas about how human experience is 'engineered' – that is, not merely augmented or supported, but shaped and generated prior to human reflection or action – by these new technologies. Thus Mark Hansen argues that new media, or 'twenty-first century media' [21CM] as he calls it, are distinct because their engineering of human experience *entirely bypasses, occurs prior to, and in sensory regions inaccessible by,* the human subject (2015, p37). In Hansen's philosophy, media are not simply 'tools' to be wielded purposefully by humans; neither are they limited to augmenting human action and the senses. These technical objects observe, collect data on, indeed 'sense' the world at a level which human subjects have no access to. A galvanic skin response [GSR] sensor might constantly observe and record this measure as a proxy for stress levels, but the wearer him/herself has no access to such 'machinic sensibility' (i.e. its ability to sense and collect data on the world) – and, importantly, could *never* access something like GSR in real time through its own sensory faculties.[28] 21CM yield data that is qualitatively beyond human experience and quantitatively beyond human grasp (something we typically call the problem of 'big data') – leading to new mediative structures for managing this surplus. This situation yields, Hansen argues, a "dispersed,

[28] GSR is a part of *continuous* variation in skin conductance – a variation that is known to be sensitive to human activity (such as differences between sleeping and highly active states), but cannot be detected by the conscious subject except in extreme cases.

environmental, non-subject-centered subjectivity" (ibid., p87) whose conscious experience is always the product of infiltration by forms of technical engineering. Variations upon this theme have been floated by other scholars, often in terms of the (qualified) agency of technical objects. The idea is that media can and do function *totally independent of* human subjects (e.g. Parikka 2011; Hörl 2015); that technology is not just an extension of man, but produces and operates *inhuman* processes (Zielinski 2006, p6). The price or consequence of recessivity is knowing but not knowing for myself, sensing but not sensing for myself.

Taken wholesale, such a narrative would place the Snowden Affair as part of a broader shift towards machinic sensibility, carried through by the massive, automated dragnet surveillance technologies. But we should be cautious about such grand historical narratives. After all, there are many pre-21st century, pre-electronic technologies that similarly undercut and bypass human sensibility. Friedrich Kittler's famous analysis of the phonograph (1986) describes precisely how sound becomes recorded and manipulated as physical waves and noise, rather than any kind of articulation. Each 'primitive' technological creation, like the hammer or the chair, is already a material-semiotic figuration (á la Haraway 1991) of processes, intentions,

power relations that offer the pharmacological bargain of extension and absence (also see Scarry 1985). The point is not that recessivity is entirely novel, but that the arrival of new media technologies entails the reorganisation of specific recessive process. In the context of the Snowden Affair, this involves the ambiguous functions pegged onto state surveillance, which becomes at once a breakthrough in knowledge production and a new source of secrets and speculation.

***

And so we turn to the question of how recessivity plays out in this context of automated, electronic, dragnet surveillance technologies. The recessivity of the Snowden files is fundamental to both the *object of surveillance* – that is, what surveillance seeks to know, to predict – and *surveillance itself as object* – as problem, as something to be known. In other words, the recessivity of electronic dragnet surveillance is not merely an artefact of the emergent conditions of the Snowden Affair, but grounded deeply in how surveillance had been defined and problematised in the post-September 11 years.

First and foremost, there is the object *of* surveillance: the recessive, elusive thing that necessitates surveillance as a technology of knowledge production. Surveillance is about rendering knowledgeable that which prefers to remain secret. In the case of NSA surveillance, this object is, of course, terrorism. Years before this new generation of surveillance could become something to be defended or attacked in public, the NSA was making its case to the rest of government that terrorism had become radically unpredictable and diffuse, and that this qualitative transformation of the danger faced by America required a new paradigm in surveillance as well. In October 2002, a joint House/Senate Intelligence Committee Hearing (which was made public) heard a Joint Inquiry Staff statement (Hill 2002), reflecting on counter-terrorism efforts between 1993 and September 11. It presented a clear narrative of terrorism's evolution in the 90s, from state-supported, limited (targeted) casualty attacks to stateless, flexible, more secret, more meticulously planned, indiscriminately high-casualty attacks. This "new breed of terrorists practicing a new form of terrorism" (ibid., p6) was already being identified within the intelligence community at least as early as the mid-1990s. The statement cites a July 1995 National Intelligence Estimate speaking of violent, generally Islamic, non-sponsored terrorists. (ibid., p7) The U.S. State Department's annual Country Reports on Terrorism (formerly

Patterns of Global Terrorism report) also indexes this shift in thinking: whereas state sponsorship is the key explanation for rise and fall of terrorist attacks in the early 1990s, the reports placed a progressively greater emphasis radical Islamic groups (US Department of State 1996), 'freelance, transnational terrorists' (1997), and eventually, 'loosely organised, international networks of terrorists' (2000).[29] The rise of 21st century dragnet surveillance was thus predicated on the identification of what I call here 'New Terrorism' – although this paranoia, once again, recalled even earlier fears about the unpredictable and untraceable infiltration of communist threats in the mid-20th century (see Melley 2012).

The response to September 11 by many top figures in the NSA and the executive branch of the government catalysed this perception of 'changing, increasingly elusive terrorism' into a realist injunction to surveillance. The simmering, longer-term idea that terrorism was slipping out of the U.S. state's predictive grasp now became a forceful statement of external, objective necessity for indiscriminate observation. The first major post-9/11 effort, the

[29] In the late 1990s and early 2000s, of course, this more flexible enemy at least had a clear organisational designation of Al-Qaeda. But as 'lone wolf' attacks grew in prominence, and Al-Qaeda itself declined in its singular status (through the death of Osama Bin Laden, the rise to notice of other groups like ISIS/ISIL/Da'esh and Al-Shabaab), the enemy as perceived became truly granular and distributed.

ill-fated 'Total Information Awareness' program, stated as much: "there will always be uncertainty and ambiguity in trying to understand what is being planned" (Poindexter 2002), it was argued, but given the largest possible collection of data, the terrorist's 'unique transaction signature' can be extracted. Knowledge is possible – as long as you have 'all' the dots on hand (Harris 2010, p147-8). The program thus promised biometrics analytics (HID); semantic analysis of text (TIDES); speech-to-text conversion for collecting and analysing auditory communications (EARS); and of course, the Big Ass Graph. Metadata surveillance wasn't a luxury; it was just what you had to do to keep up with the reality out there.[30] Knowledge production had to keep abreast of new uncertainties, new dangers. In the public domain, one popular explanation for 9/11 became the intelligence agencies' failure to coordinate and 'connect the dots' (Hill 2002; also see Harris 2010). Although this was criticised by some as simplistic (e.g. the 9/11 Commission Report (2004)), such debriefings helped present a sense of necessity for surveillance that was more comprehensive, more powerful, more, more, more. The political and material

[30] This hunger is not simply a default modality for intelligence agencies. Mike Hayden, then Director of the NSA, was hesitant to support metadata surveillance tools like ThinThread before September 11 due to an entrenched sense of caution since Watergate (Bamford 2008). Although metadata collection and mass surveillance of communications media existed in various forms throughout 20th century America, the specific rise of the kinds of tools Snowden has exposed came as a result of a heightened sense of uncertainty and danger, and correspondingly, a perceived need for revolutionary solutions.

consequences of this narrative included the creation of over 70 Fusion Centres[31] nationwide; a vast monetary injection rejuvenating the NSA, which before September 11 had been suffering from a slow decline in funding and influence; and a series of 'collect em all' online surveillance solutions, from Total Information Awareness to Snowden-era programs like XKEYSCORE and PRISM. The American public was told that it was necessary to turn to bulk collection, mass surveillance, indiscriminate monitoring, more than ever – because there is an objective, realist uptick in the danger of terrorism, and its qualitative transformation to spread its seeds more pervasively and covertly than ever. This narrative of 'new' terrorism would persist in subsequent years, becoming increasingly centred on the figure of the 'lone wolf'.[32] In 2015 as much as 2001, a flexible threat, a fluid world, was seen to demand a totalising gaze.

Such a worldview did not emerge from a vacuum. The pairing of national security and total surveillance has numerous predecessors on both sides of the Cold War, from McCarthyist America to East German intelligence.

---

[31] Fusion Centres are physical hubs for consolidating CCTV, license plate reader and other surveillance information from local and federal, private and public sources.

[32] Consider, for example, Barack Obama's designation of mass shootings by unaffiliated individuals as the direct heir to 'complex, multifaceted attacks like 9/11' in the wake of the San Bernardino shootings in December 2015 (Obama 2015).

Indeed, the Stasi articulated their problem of 'too much data' in much the same terms the NSA would decades later; joined by a wide network of unofficial informants, they took the strategy of 'collect first, analyse later', and found that too much data was interfering their ability to produce useful knowledge (Angwin 2014, Wensierski 2015). Alongside this political heritage, New Terrorism was part of a broader problem posed by the Internet and its upsetting of traditional boundaries for communication and public formation. In this same period, the maturation of the Internet as a popular technology produced vast crowds with communicative and informational capacity, such that many traditional ways of 'knowing' this multitude as a population was felt to be obsolete and inadequate. Even as data-mining technologies offered corporations and advertisers a new hope for knowing the population as consumers, the same set of technologies were being taken up by agencies like the NSA as a way to keep up with the networked population of potential terrorists. These connections are not meant to imply a centralised intention governing the rise of data-driven solutions across states and corporations. Previous studies of such broader 'rationalities' have shown that new epistemological tools and principles often emerge as little 'islands' (Foucault 2006, p4) – localised solutions to local problems that, when viewed retroactively, turn out to 'invent' similar ways of doing using similar kinds of

techniques.[33] In this case, the turn to call big data, both state and corporate, was intended to address a significant and new unknowability in the population, an unknowability that was threatening to turn the masses into a threatening entity (a 'hotbed' of terrorists and dormant lone wolves, a consumer population unable to be monetised). Like the fear of the urban multitude of strangers that inspired 19th century crowd psychology, perceptions of an uncontrolled and unknown proliferation was central in the post-September 11 evolution of surveillance as knowledge production.

In short, post-9/11 electronic mass surveillance developed, and justified itself internally and externally, by invoking a new kind of uncertainty in the world out there; the upgraded, twenty-first century bogeyman of the transnational Muslim extremist (and, increasingly, the radicalised lone wolf). Certainly, terrorism's modus operandi has always been to be unpredictable, to function in ways that cut underneath the system of expectations and defences erected by conventional warfare. But the older figure of the state-sponsored, organised terrorist suddenly appeared relatively stable, relatively easier to

[33] Histories of science and technology have similarly identified many broader epistemological frameworks – for instance, the definition of 'sound' and 'noise' (Thompson 2002) – as emerging through disparate, independent efforts to solve local problems that later find connections and similarities. This perspective is, of course, emblematised by Thomas Kuhn (1962) and Ludwig Fleck (1979).

'know', in comparison with the new world order. This is the first sense in which Snowden-era surveillance was *founded* on a projection of recessivity.

An important corollary is that this generation of surveillance *requires* an unknowable and amorphous terrorist threat as its object, as its *raison d'être.* An epistemological solution often impresses its necessity precisely by emphasising the danger of its other. As discussed in Chapter 4, the now-familiar ideals and practices of scientific objectivity arose in tandem with a new conceptualisation of the scientific subject. In our case, justifications for surveillance's necessity and efficacy was dominated by future-oriented, potentialist arguments that leveraged the seemingly inexhaustible and irreducible threat of New Terrorism in order to persuade the public. This is, in fact, a rather tricky case to make: how do you assert the increasing unknowability of the Al-Qaeda bomber or the lone wolf, and at the same time, prove that new surveillance technologies render them significantly more knowable and preventable? The justifications themselves took on a recessive quality, pointing to the unknowable as the ground for verification. The idea was that surveillance is justifiable not because these particular people we have monitored ended up trying to bomb the White House, but because anybody (that is, everybody) *could* one day decide to do so, and *if* such a thing

happened in the future, we *would* be able to stop them. The non-occurrence of a posited event thus acts as an unfalsifiable proof of surveillance's necessity, while the fundamental unknowability of the new terrorist requires that surveillance continue indefinitely and expand indefinitely. We will encounter specific articulations of such reasoning in Chapter 3. For now, suffice to say that the unknowability of terrorism is not just the enemy against which surveillance forms an epistemological bulwark; this technological solution has built its claim to efficacy and validity upon that same attributed uncertainty.

Second, there is surveillance *itself* as recessive object. This secret practice was concealed, to various degrees, from the public, from Congress, from the judicial branch (save the FISC[34], which itself remains secret). This system was designed to ensure that an individual will never be able to confirm whether and how he/she has (not) been surveilled. Surveillance required a vast material stratum – server farms, tens of thousands of employees – yet these too were concealed in access-restricted, remote locations. And yet, as we have seen, the world could not stop talking about (and being told about) it.

[34] The Foreign Intelligence Surveillance Court is a curious creature. While it exists solely to provide judicial oversight to surveillance activities, the court's proceedings are held in secret – meaning no victim or concerned citizen may raise any kind of objection – and the court itself, by its own admission (Leonnig 2013), does not have the ability to audit intelligence agencies' activities. The Court thus operates by the surreal logic of 'given what the NSA have told us about what they are doing, we judge that it is legal/not legal'.

"Surveillance", "mass surveillance", "metadata", "bulk collection" – these buzzwords index a public relationship to a secretive technological apparatus that continually announces (or is made to announce) its existence and significance, but in doing so, stresses its own fundamental unknowability. A part of this is down to the basic epistemological and technological principles that define NSA surveillance as a practice. Electronic surveillance's claim to objective knowledge is founded on the subject being unaware that they are being watched in any specific way. The point is to capture the secret truths of individuals that they would conceal and mask in the eyes of others. To contrast this to a more 'traditional' form: American police surveillance, especially with regards to poorer black communities from the 1970's onwards, have adopted strategies by which the targets are made to constantly encounter the naked violence of the state: house raids, summons to court, loud patrols, pat downs, urine tests (e.g. Goffman 2014). In that modality, surveillance is in your face (and all over the rest of your body): the point is not only to ferret out undesirable aspects of the population, but to impress upon you the power the police has over you. You may never know if an NSA agent has read your e-mail (or if their system has automatically collected its metadata), but you will certainly know if the police has questioned your family. There is no simple binary here, of course. Police violence is also a way

to breed docile subjects that voluntarily discipline themselves in remembrance of authority – and it is not inconceivable that digital surveillance in the future could similarly visibilise itself.[35] The point is that electronic surveillance as we know today relies on a certain recessivity to do its job, and that such configurations of how surveillance *appears* to the public has repercussions for what kinds of affective and epistemological relations we are likely to form with it. We find a formally comparable shift in Foucault's history of discipline and punishment (1995), when it documents the passage from the spectacular public punishment of the regicide Damiens to the exhaustively documented, examined, trained bodies of the carceral archipelago. There, one of the key differences was how punishment was meant to appear unto subjects' affects and reason. With Damiens, the design was that subjects would carry away the gory scene with them, back to the streets, alleys and homes where the state could not follow (including Foucault's famous 'margins of tolerated illegality' (ibid., p82-3)). The body of the condemned made appear a presence of the sovereign, and reminded subjects of their own vulnerability to that state sovereignty. In 18th century prisons and workshops, we find a structural production of docile bodies and

[35] Indeed, there is constant speculation that now Snowden has brought so much scrutiny to agencies like NSA and GCHQ, the organisations are now seeking to use this new visibility to their advantage. For instance, the NSA has sought to control the release of some information on its own terms through the IC on the Record website.

souls across a local *totality* of time and space, such that the subject would always already be classified into deviant and normal (at least, ideally). In the time of Snowden, a recessivity is built into the very design of the surveillance apparatus, because its basic operation depends on that withdrawal. This is part of the reason that uncertainty persists even after the leaks. At least Orwell's Big Brother had the courtesy of telling you exactly how it is watching you everywhere, blazoning its aesthetics all over the urban environment. Today, we are left to wonder.

Recessivity is thus fundamental to how the Snowden Affair, and beyond that, state surveillance in the age of 'New Terrorism' has been defined, justified, problematised, condemned. The recessivity of documents is only one aspect of a general situation wherein expansive bureaucracies, automated technologies, 'big' databases too big for humans to grasp, the apparent unknowability of New Terrorism, and the desire for a 'raw', objective truth about the population all combine to produce felt uncertainties. What an incident like the Snowden Affair does is grant a heightened visibility and public significance to a latent and structural paradox, because involved parties are pushed and tested on their claims to knowledge so strongly. We may now proceed to the other recessive objects populating this conflict, and

in doing so, examine the different, contingent ways in which the public, the state, the terrorist, and surveillance technologies are arranged into recessive relations.

THE LONE WOLVES

> He was a dude you could always just vibe with. He liked *The Walking Dead* and *Game of Thrones*. He couldn't have been sweeter. He smoked a copious amount of weed. He won a $2,500 dollar educational scholarship. He was one of the realest dudes I've ever met. He was just superchill. He was smooth as fuck. He was not a loner. He's not anybody *like that.* I mean, he was quiet – but not in an alarming way, he was just soft-spoken. He's a Muslim, but not so religious. He was so, so normal, no accent, an all-American kid in every measurable sense of the word.
>
> He stopped listening to music. He quit drinking and smoking pot. (He started praying more, and visiting Islamic websites.) He became anti-fun. (He went to Dagestan for six months.) He grew a beard. He criticised U.S. foreign policy. "There are no values anymore," he once said. He would start failing classes. In the aftermath, we know that we never really knew him. The contents of his closely guarded psyche may never be fully understood. It's weird, they all agree. But I can't feel that my friend is a terrorist. That Jahar isn't, to me.

***

Such were the words of friends, acquaintances, investigative reporters, professors and police workers – the authoritative 'experts' in such a situation

– about Tamerlan and Dzhokhar 'Jahar' Tsarnaev.[36] They were the 'Boston bombers' – two Chechen-born, long-time Massachusetts resident brothers who exploded pressure cooker bombs at the Boston marathon just two months before the first Snowden leaks. And in the wake of their actions, there was a frenetic public effort to narrativise, rationalise, render knowable, this apparent cohabitation of radical terrorism and 'normal' American life. Where Tamerlan had already become distant and conservative after the premature end of his boxing career, witnesses emphasised how Dzhokhar would watch HBO shows, smoke weed with (white, well-adjusted) mates, enrol in extra-curricular activity – as if such things should have marked him as a normal American citizen, and more than that, *a 'normal' human being whose thoughts and emotions we can thereby predict.* As if to say: listening to the same music I do might not dictate his political or religious outlook, but at least I know that, by the broadest of brushstrokes, he will see the world as I do, that he will value another human's life as I do, that he will not be fooled completely by conspiracy theories, that he will see September 11 as tragedy and not as farce (Jahar allegedly subscribed to the theory of 9/11 as an inside job). In the same

[36] Each comment was sourced from such an 'expert' as reported in the media (Stout & Goodison 2013; *CBS News* 2013; Coffey et al. 2013; Henderson 2013; Reitman 2013), with minor grammatical corrections for consistency. Put together, they depict not a clear understanding of 'Jahar' or his brother Tamerlan, but the general contours of a question, an unknowability.

way that America's presidential candidates stuff themselves with hot dogs on the campaign trail, there is an identification of a basic humanness that allows us to try and say this person is safe, this person is not a criminal, terrorist, serial murderer, child molester. This, as shown in the phenomenological tradition (for instance, see Husserl's assimilative apperception (Ricoeur 1967, p129)), is how we try and overcome our fundamental solipsism. We can never truly know what people *really* think about Islam, America, race, war, deep inside; but we still try to identify this 'basic humanity' – to be able to say, this person is like us, and we can trust that he will not be this radical, terrifying, and in some ways, *inhuman* danger – not if he can sit and vibe with us like this, not when his English is so perfect. Except, of course, he *was*.

Individuals like the Tsarnaevs were so problematic for security actors and observers because they confounded the perennial (and never quite successful) effort to cleanly categorise enemies from allies, threats and suspects from normal citizens. When the killer comes from the desert, armed with violent motive, but also trained, equipped, and identified by a recognised group, understanding comes readily: this individual's being is *entirely, and from the beginning*, coterminous with violent terror. The category *is* him (and it is almost always a 'him' – statistically so, and especially in the public

imagination). To know 'Jahar', on the other hand, requires a narrative of a switch, a doubling. He must have begun as a benign, *real* American – and then somehow changed into a killer. Something must have made him trade pot for bombs. Or perhaps he had always harboured, in the schizophrenic folds of a duplicitous soul, a Jihadi mind. This has been called the problem of the Double – an ancient figure of folklore which, in this modern rendition, describes the infection of the unknown, the other, the dangerous, in precisely what we try to cordon off as safe and predictable (Szpunar 2015).[37] Here, the problem of *security* – of guaranteeing the safety of certain peoples, areas, types – becomes intimately tied to the problem of *knowing.* The dogged efforts to resolve Jahar's psyche into a neat narrative of belonging, or to locate the exact moments and incidents that might have 'caused' his transformation into terrorist, reflects this idea that a terrorist that cannot be known cannot be predicted, and thus presents an unknown danger with a powerful absent presence.

But why were the likes of Jahar so difficult to know, to predict? One problem was that they had not belonged to any terrorist organisation, no existing

[37] This shift is also germane to the history of how Westphalian nation-states have demarcated the nation from its enemies. The shift of the locus of terrorist danger from the outside to the inside replicates the early 19th century transition of the notion of 'war' from an external affair to a broader set of conflicts marked by the Other's infiltration into the inside (Foucault 2003).

network of suspicious acquaintances. The post-9/11 period has seen a series of high-profile attacks by such individuals, which the media, academia, and the state in turn characterised as the *lone wolf*. While the label enjoys no single definition, and is often criticised as ill defined (e.g. Spaaij 2012), we might point to a widely used description from the intelligence firm STRATFOR: "a person who acts on his or her own without orders from – or even connections to – an organisation" (Burton & Stewart 2008). The label itself originated in the 1990s with Alexis Curtis and Tom Metzger, two white supremacists who espoused the 'evolution' of their struggle from organised, and therefore easily identifiable, groups to individuals that could 'act alone and leave no evidence', 'act silently and anonymously', and thereby preserve the secrecy of themselves and others.[38] By the later 2000s, the Lone Wolf had become a prominent figure in narrativisations of domestic terrorism; in 2009, the US government announced the so-called 'Lone Wolf Initiative' (also see Michael 2012). By then, the problem was already being defined in terms of 'knowing' the deepest and thus most unknowable aspects of the individual's psyche: "How do you get into the mind of a terrorist?" (Fields & Perez 2009) The figure of the lone wolf was seen as part of a historical trajectory, part of the

[38] For more, see (*Aryan Vanguard* 2012; *Anti-Defamation League* n.d.). This development had its own context: far-right leaders like Louis Beam in the 1980s had already been touting 'leaderless resistance' as the next step to their struggle.

turn to New Terrorism: although much terrorism remained tied to clearly identified organisations like Al-Qaeda, the lone wolves depicted a new outbreak of unpredictable and solitary violence. In other words, the figure of the lone wolf marks a qualitative shift in imaginations of terrorist danger. As we can see with Dzhokhar Tsarnaev, the uncertainty that plagues the lone wolf concerns not simply the generic threat of terrorism or violence, but a more viral danger: a diffused vulnerability to the smallest of human units, where just a single outwardly normal youth is enough (Simon 2013). The lone wolf, then, is a ghost, a figuration, of that which lies outside the epistemological systems of surveillance, security and suspicion. Like the residual in statistical analysis, it expresses the indeterminate danger that remains after every effort to predict and prevent. This fear of an indiscriminately distributed *potential* for terrorism would feed into the idea that state surveillance, too, must become more comprehensive, more indiscriminate, and infinitely data-hungry.

The lone wolf thus names the apparently new and radical uncertainty appended to the traditional danger of terrorism. Yet at the same time, the lone wolf is the object of academic, state and popular effort to 'figure it out' – to fold this alien threat back into the domain of the knowable. After all, policy,

deliberation, or even a sense of control is difficult when one can only speak of unknowns. To leave the lone wolves entirely mysterious is to continue producing a sense of vulnerability.[39] The result is that even as the lone wolf is a recessive object, a name standing in for the unidentifiable, it also becomes the locus for a belief in knowability. High-profile attacks in the early 2010s[40] have been met by studies which seek statistically significant, and thereby predictive, variables for the lone wolf. The kinds of questions they *begin by asking* already express the hope that surely, like other dangers and threats, we shall be able to render the lone wolf knowable: 'what are the demographic characteristics of the lone wolf?' What are its ideologies? How are they different from other groups? (Gill et al. 2014) Such questions, however, tended to yield results that testify to the sheer genericity and improbability of the lone wolf. One sampling (ibid.), for example, shows that lone wolves in the United States have a higher than populational norm chance of living alone, have changed their address and/or lost their job in the 12 months preceding the attack, and records of criminal behaviour or mental health

[39] This is a structural, epistemological variant of what, in an affective register, Lauren Berlant calls the 'unbearable' (Berlant & Greenwald 2012).

[40] The most prominently covered tragedies – Andres Breivik in 2011, the 'Boston Bombings' in 2013, Charlie Hebdo and Bataclan shootings in 2015, the San Bernardino shootings in 2015 – were joined by a series of attacks upon American military and government buildings (Little Rock recruiting office 2009, Fort Hood 2009), Muslim / anti-Muslim sites (an attempted bombing of a Florida mosque 2010), and others, such as attacks on Planned Parenthood in 2010, 2012 and 2015.

problems. Yet each of these factors are possessed by less than half of these proven lone wolves. Should the state put under watch a man who loses his job and separates from his partner? Or a man whose problems with depression has put him out of his last job? Similarly, the studies seek to isolate lone wolves' 'unique psychological and motivational factors' (Eby 2012, p11), typically founded on a 'faulty' – that is, non-normative – environment. Hence one study insists that Timothy McVeigh, Ted Kaczynski and Eric Rudolph are united by a 'repeated failure' to belong (Springer 2009), while another speaks of a 'difficult childhood' and 'changes in personal behaviour' (Kaati & Svenson 2011). Of course, many criminals are retroactively analysed for psychological problems in order to explain their behaviour – the idea being that *something* must have been wrong with them for this to happen.[41] Following the fall of Nazi Germany, for example, the victorious Allies conducted Rorschach tests on the eight most 'serious' surviving Nazis, including Hermann Göring and Adolf Eichmann. There, too, the results were inconclusive: no 'Nazi traits' that could predict totalitarian depravity could be identified (Lemov 2015). Whatever formal and general property extracted from existing lone wolves (e.g. experience of poverty, divorce, crime in the

[41] Even *excessive* empathy can be conceptualised as a psychological fault: one study (McCauley & Moskalenko 2014) suggests that individuals can go from a 'normal', happy life to violent action because their latent, invisible radical opinions were catalysed by unusually extreme empathy (for instance, with something they have seen in the media).

family during childhood) ultimately proved insufficient to identify, predict or explain the lone wolf.

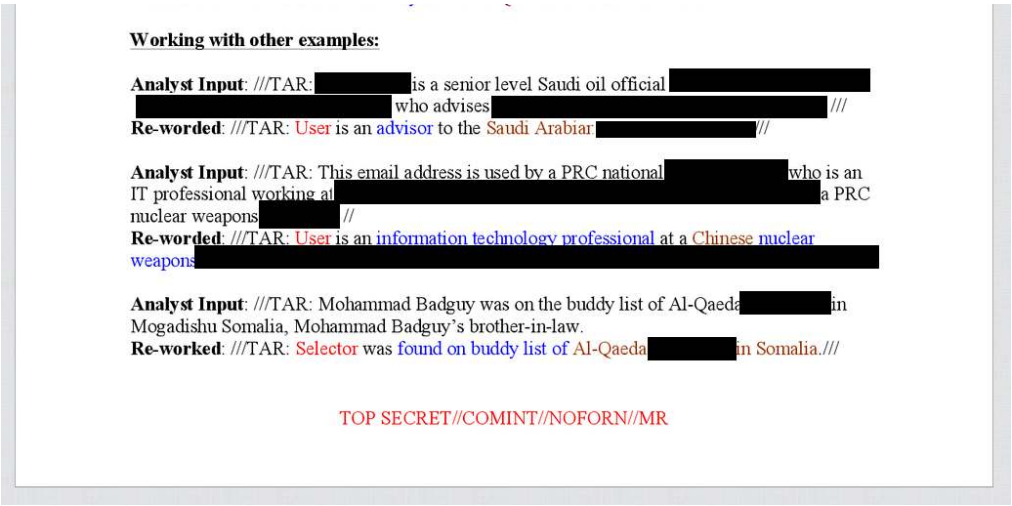
In short, the effort to know yields little in the way of tell-tale signs, only 'many weak signals' (Brynielsson et al. 2012) – signals that are too weak for traditional thresholds of suspicion or prediction. This is also consistent with the public presentation of lone wolf threats as a paradox: on one hand, so many signs seem so obvious now, but on the other hand, they never seem to add up to something concrete enough for prediction. Jahar Tsarnaev was failing his university courses, *but,* the story goes, he was popular with his Cambridge friends. This lack of 'clear signals' retains the lone wolf in a state of nonspecificity, and visibilises the failures of efforts-to-know, and even raises the spectre of total randomness, total unknowability. Instead of the ISIS member, the Al-Qaeda operative, the card-carrying white supremacist, the lone wolf expresses the latent potential for *anybody to become a terrorist* – a structural paranoia that is formally parallel to the paranoia of surveillance as conspiracy and of New Terrorism writ large. Not needles in a haystack, but that every piece of hay could become a needle when you look away. (This 'anybody', of course, becomes recharacterised, approximated, to rule out certain demographics – say, the high earning, well educated white male. We

will return to this paradox below.) In other words, even as studies describe 'weak signals' everywhere (Brynielsson et al. 2012), a constant and pervasive war of ideas between terrorism and the government (McCauley & Moskalenko 2014, p72), they also report that many lone wolf killers remain mysterious in their motivations and ideological allegiances, even after the act (Spaaij 2012). Thus, across academic and policy analysis (Bakker & de Graaf 2010; Eby 2012; Gill et al. 2014; Spaaij 2012) and popular media coverage (e.g. of Man Haron Monis, instigator of the 2014 Sydney hostage crisis), there is an acknowledgement that the lone wolf does not boil down into a single profile, personality type, or even definition.

The lone wolf, then, is a figuration of a particularly diffuse unknown. A cipher for the inevitable uncertainty, the residuals, the margins of error, that defy surveillance's vision of total knowledge. And yet, recessivity is always a pairing: even as the lone wolf is a figuration of the unknowable, this figuration is part of an extensive effort to nevertheless describe, characterise, classify. Assumptions and archetypes are smuggled in in disavowed form: 'the lone wolf is impossible to predict or identify, but even so…' In this way, the 'anybody' of the potential terrorist is reduced down into, in this period, the Arab and Muslim (e.g. McCauley & Moskalenko 2014; Pantucci 2011).

Broad geopolitical perceptions thus find their way into working approximations of a technically unpredictable group – to the point that 'recent conversion to Islam' alone (rather than religious fundamentalism in general, or specific extremist doctrines like Salafi jihadism) become cited as possible predictors for lone wolves (Kaati & Svenson 2011). In fact, many of the more prominent attacks by Muslim extremists in this period were by members of organised groups: September 11 was organised by Al-Qaeda, the November 2015 Paris shootings executed by ISIS operatives. In at least one case (of Man Haron Monis), Islam was most likely a ploy for attention, and not the cause for which the attack was carried out. And until the last fifteen years, lone wolf attacks were more commonly by white supremacists than Muslim extremists (Spaaij 2012). To be sure, the threat of terrorism by Muslim extremists is very real for the United States. The point is that this relatively specific figure of the Muslim extremist starts to conflate with, and stand in for, the allegedly unknown lone wolf. This is exemplified by Mohamed Badguy, a fictional name used in NSA slides to provide examples of the targeting process (Gellman & deLong 2013b; see Fig.2). He is joined by a slightly less blatant cousin, "Mohammed Raghead", which the NSA used as a placeholder for surveillance memo templates (Davidson 2014). The mainstream media has responded to the rising number of lone wolf attacks in post-9/11 America in a

similar way, though wielding a more varied set of stereotypes: Muslim extremists are joined by anti-Muslim extremists, while almost every lone killer is immediately dissected for signs of mental deviance. Scenarios, exemplars and simulations reveal much about what kinds of assumptions and provisional designations 'stand in' for the as-yet-unknown.



Working with other examples:

Analyst Input: ///TAR: [redacted] is a senior level Saudi oil official [redacted] who advises [redacted] ///
Re-worded: ///TAR: User is an advisor to the Saudi Arabian [redacted] ///

Analyst Input: ///TAR: This email address is used by a PRC national [redacted] who is an IT professional working at [redacted] a PRC nuclear weapons [redacted] //
Re-worded: ///TAR: User is an information technology professional at a Chinese nuclear weapons [redacted]

Analyst Input: ///TAR: Mohammad Badguy was on the buddy list of Al-Qaeda [redacted] in Mogadishu Somalia, Mohammad Badguy's brother-in-law.
Re-worked: ///TAR: Selector was found on buddy list of Al-Qaeda [redacted] in Somalia.///

TOP SECRET//COMINT//NOFORN//MR

Figure 2. Mohammad Badguy.

Let us return to 'Jahar' Tsarnaev. The lone wolf as a problem of (un)knowability is central to the problem of the lone wolf as 'double', in the sense that the crisis of the threat as double is a crisis of *intelligibility.* As Jasbir Puar and Amit Rai (2002) show, the West's discourse on the terrorist is often that of the human *monster*: an ancient frame for the disturbing entry of fundamentally unintelligible and strange deviance into the normal and the internal. The unknowability of the lone wolf is problematised precisely

because it threatens to collapse the erected boundaries between us and them – a boundary that is never perfect to begin with. Every 'normal American' trait possessed by Dzhokhar Tsarnaev challenges the epistemic techniques at hand. In other words, the lone wolf's recessivity is a liminal and transgressive thing, because it cheats the boundaries between what is epistemologically, and politically, *included* and *excluded*. To speak a bit of Foucault, any regime of knowledge is defined by what it considers *know-able* and what it renders invisible and unsayable. This is not the distinction between what statements are accorded the status of truth or falsehood, but what kind of statements are even eligible for the claim to truth in the first place.[42] Judith Butler (1997) derives from this a matrix of inclusion/exclusion: to be a subject is not necessarily to be what dominant power relations tell you to be, but to define your being in its terms. The price of refusing this bargain is not to become a resistant or alternative subject, but to become *unintelligible.* Neither true nor false, but not even a statement to begin with. As a label, an object of study, a category, the lone wolf describes American society's effort to respond to the entry of the excluded – a being which transgresses the basic obligations of citizenship – by seeking ways to integrate this unknown into grids of

[42] Though this is true of Foucault's corpus as a whole, here I am referencing in particular his later efforts at 'alethurgy': a study of what people say that is true, but what are the conditions under which such speaking is *seen to be possible* (Foucault 2014).

intelligibility. With the Snowden files, we emphasised how the recessivity – the combination of appearance and dis-appearance – prevented a fuller sense of knowing, opening up space for speculation. With the lone wolf, we find that recessivity permits a technically unknown thing to be brought in for examination and analysis.

In short: the lone wolf is about rendering the unknown visible, a matter of concern, a problem – and in doing so, using that very figuration to smuggle in working assumptions about what that unknown might be. This paradox of recessivity is precisely what renders the label *useful*: that is, something that we can make predictions with, that we can use to produce narratives, to at least gesture towards a future point of predictivity and thereby safety. The lone wolf is like a variable in an equation: the x and y could be anything, and the point is to try and construct a structure, a logical scaffolding, that allows this specifically unknown object to become usable for running calculations, assessing the situation, making decisions. It illustrates the ways in which uncertainty is not necessarily knowledge's antithesis, but an ingredient for provisional and practical kinds of knowing. The unknown is not a pure void of meaning, but a space for filling in.

***

In the wake of the Snowden leaks, one of the most frequently cited arguments in defence of NSA surveillance was that those who have done 'nothing wrong' have nothing to fear (see *Domestic Surveillance Directorate* n.d.; Fig.3). The question is, of course, what counts as 'nothing wrong' in a surveillance epistemology which defines its enemy as a collection of 'weak signals' embedded within its citizens, and defines its mission as preventing criminals before they can become criminals (see Ledgett 2014; Massumi 2007) – to the point where agents are on record as encouraging, equipping and instructing individuals in order to arrest them (see Chapter 3, 'Fabrication')? For an individual to insist that they have done nothing wrong is rather besides the point; the politico-epistemic problem here is how, by whom, the definition of 'nothing wrong' becomes modulated. Most crucially, where the debate revolves around recessive objects that are openly acknowledged to be partly speculative and uncertain, the normative assumptions governing those definitions can become difficult to recognise. In an analogous case, Torin Monahan (2010) shows how intensive surveillance in Phoenix, Arizona public housing units were justified – by wardens as well as some residents – by the same rationale of 'nothing to hide'. And this very mode of reasoning,

Monahan shows, produces an implicit classification whereby certain kinds of foreign Others are presumed into 'bad types' or 'bad sorts', often without surveillance itself needing to produce any evidence. What is at stake is the unarticulated definition of the 'normal': what a normal citizen expects, what a normal citizen does in his/her private spaces (though of course it is supposed to be nobody's business), what a normal citizen should be (un)comfortable with.

Figure 3. A parody of the Utah Data Centre.

Uncertainty and unknowability are, just as much as knowledge, subject to social processes of visibility and definition. To 'know' is often to forget the unknowns that it is founded on, or rather, to forget the conventions that have been erected to translate and approximate the unknown into the 'sufficiently

known'. Recessive objects help us perform this task, even as they draw our attention to the uncertainty and the unknown, a 'gap' that they cannot quite close. But the relation of appearance/disappearance, presence/absence we have charted here is far from the only possible configuration. The very same kinds of technologies and epistemological principles can and do end up with a different arrangement of projected uncertainties. The next chapter examines how the source of unknowability shifts away from the terrorist 'out there' and inwards unto the self. While the NSA was bulking up its dragnets, personal experimenters and commercial start-ups were applying such technologies to the booming field of self-tracking. There, we find a formally comparable, but substantively different, configuration of knowledge and uncertainty – one which challenges the place of human agency and experience in the process of knowing.

2. Data's Intimacy.

> "Walking, sleeping, talking: it's the stuff of everyday life. Add sensors that track all of it, and suddenly everyday life becomes an opportunity for knowledge." (Wingfield 2013)

You sleep. A thin rectangular strip, slipped unobtrusively under the bedsheet, senses your arrival; your movement; your resting heart rate; respiration cycle; and more. The smart sensors on the strip collect the data and transmit through WLAN to the cloud for analysis (Leppäkorpi 2011). When you wake, your consciousness is greeted by a numerical sleep score on the smartphone app screen; a simple distillation of the many data points, and their estimated relationship to sleep quality, into a score out of a hundred.

Beddit, released to the public in 2014, joined a wave of much hyped – and sometimes commercially highly successful – technological solutions for self-surveillance and analysis that began to reach Western consumer markets in the 2010s. This device exemplifies a promise that is central to many of these instruments: a promise to mine the body for traces that the thinking, experiencing subject is incapable of sensing for him/herself. In Beddit's case, it is the myriad physical signals that every body emits during sleep that are

automatically collected and analysed. Though older technologies also afforded such tracking capacities, these were cumbersome and expensive, often only available in clinical contexts. (A polysomnogram, typically used in sleep research, still requires belts around the chest and abdomen, electrodes over the face and scalp, and oximeter probes wound tightly round a finger.) Technologies like Beddit thus promise to measure what the subject cannot, and deliver 'insights' about the self beyond the reach of human intuition and experience.

***

At one corner of the Herbst Pavilion, on the San Francisco waterfront, two white, blonde women were beckoning nearby flâneurs to their booth. On offer was a small, triangular device tied to a black strip, vaguely futuristic in its silver-white sheen (Fig.4). Just let it fire electrical pulses into your brain for a few minutes, they said; it can make you feel more active and productive, or if you prefer, calm and de-stressed. Several individuals were already huddled over the test smartphone, the device strapped to the temple. As I dialed up the intensity on the 'Energy' module, the strap seemed to fire rapid, stinging bursts into the head, producing a distinct 'heaty' sensation. One of the women

explained that just as you might use caffeine as a pick-me-up, this is a more direct and effective method of controlling and optimising your body and mind. My own experience, as far as I could tell, were less clear; a mix of novelty's discomfort and a certain general feeling of tension. Yet if I doubted that this device was anything more than the snake oil of the new century, this proved nothing either way; after all, a device like Thync is designed to augment and regulate the subject beneath and before consciousness and its struggles. Thync promises, through new forms of data-driven surveillance, a self-knowledge with an immediate and practical impact over how we manage and control our own selves.

Figure 4. The Thync headset.

Thync and Beddit, in fact, were both to be found at the Herbst Pavilion that day, having turned up for the 2015 Quantified Self conference. Quantified Self [QS], a community of self-tracking experimenters, was born in September 2007 amongst two *Wired* editors; by 2015, it had spread to dozens of cities globally, with annual conferences in the US and Europe. While such a community is not coextensive with the self-tracking industry or market, the overlap and synergies have been significant. Crucially, QS was a breeding ground for an evolving set of ideals and predictions that tied tools like Beddit and Thync to a futuristic vision of an individualistic, objectively known, constantly improving, data-driven human. As Kevin Kelly, QS' co-founder and a long-time evangelist for computing technologies, put it:

> The central question of the coming century is Who Are We? What is a human? […] Many seek this self-knowledge and we embrace all paths to it. However the particular untrodden path we have chosen to explore here is a rational one: Unless something can be measured, it cannot be improved (Kelly 2007).

Even as concrete self-tracking devices were slowly making their way onto the market, QS was building a community of enthusiasts and do-it-yourself tracking experimenters that coalesced around the idea of 'truly' knowing the self through objective data. Gary Wolf, the other co-founder would make the case in such terms in a widely read *New York Times* piece:

> Sometimes we can't even answer the simplest questions. Where was I last week at this time? How long have I had this pain in my knee? How much money do I typically spend in a day? These weaknesses put us at a disadvantage. We make decisions with partial information. We are forced to steer by guesswork. We go with our gut. That is, some of us do. Others use data (Wolf 2010a).

***

Uncertainty in the Snowden Affair resembled an infinitely receding horizon, a Matryoska doll without end. Whether it be the justification of state surveillance through the unpredictability of the lone wolf, or the recessive ways in which such surveillance itself becomes accessible for criticism, the problem and promise of knowing was defined precisely through the unknowns undergirding the logic of new terrorism, the systems of data-driven surveillance, and the principles of state secrecy and public political 'participation'. But what happens to knowledge and uncertainty, to the distribution of veridical authority, to the definitions of what 'counts' as knowledge, when surveillance technologies are harnessed towards the individual's personal quest for self-knowledge?

This chapter examines technological practices of self-surveillance in the early twenty-first century as a parallel development in data epistemologies. If state surveillance after September 11 directed and extended existing technological practices towards more heavily machine-automated, more persistent, more recessive systems, self-surveillance in that same period claimed two aspects in which they were 'upgrading' older technologies of self-inquiry: automation and intimacy. Across these tools, multiple stages of collection, archival, analysis and implementation would be automated through machines at an unprecedented scale. Heart rate variability or walking movements might be detected silently and autonomously; the tools might then make behavioural recommendations or directly send commands to home appliance of their own accord. This process would also cling to individuals with a new degree of proximity or intimacy. This meant not only devices close to the skin, but also devices which enter into the home or the bedroom, into the most socially invisible of daily habits, into the emotional and otherwise internal workings of the body. Hence we find tattoos embedded into the arm that senses physiological signals multiple times a second, or smartphone applications that silently monitor and extract data from sexual intercourse.

Contemporary discourse tended to bring all these together in a broad category of 'self-tracking' devices – or, taking the name of the movement, 'Quantified Self' solutions. This category itself belongs to a loose nebula of emerging instruments. In this chapter, we call self-tracking any hardware or software solution that uses machinic *sensors* to surveil individual subjects' everyday lives, from physiological signals to social habits. Such tools took the broader technological principles – 'big' data, machine learning, algorithmic decision-making – that had already transformed state surveillance and corporate data-mining apparatuses, and applied them to an everyday context of self-care. And with that technological transfer came an epistemic one. These new tools promised to uncover the kind of truths the human subject has traditionally been incapable of accessing. If state surveillance are leveraging new capacities for collecting and processing 'big' data to lay claim to greater knowledge and the elimination of uncertainty, today the public is being encouraged to surveil themselves through machines in the same way.

One important difference between state and self surveillance of this period is that whereas the NSA had already implemented data-driven surveillance at an international level, self-surveillance remains a few years behind the curve. By the early 2010s, self-tracking was part big business, part big dreams.

Market estimates pegged the sale of 'wearables' – from fitness bands to smartwatches – at 15 billion USD in 2015 (*CCS Insight* 2015); the third quarter alone had seen over twenty million units shipped worldwide (*International Data Corporation* 2015; also see Lupton 2013a).[43] By then, a number of high-profile, relatively simple self-trackers had achieved millions of sales and a general public awareness. Fitbit, a wristband primarily based on its accelerometer sensor for movement detection, began to normalise a more data-driven and persistently surveilled attitude towards exercise. Meanwhile, the Apple Watch introduced a broad suite of sensor-based recommendations to its several million users. The Watch's inclusion of optical heart rate sensors, pressure sensors and more was an extension of the important precedent set by the popularisation of smartphones in the late 2010s. Following the Apple iPhone in 2007, the spread of smartphones, stocked with an ever increasing number of sensors,[44] helped equip large portions of the US population with a shared baseline of tracking functionalities at the hardware level. All this was catalysed by a convergence of relevant technological advancements. 'Smart

[43] Similarly, Deborah Lupton (2013b) argues that by 2012-13, the early frame of 'weirdos' and eccentrics in media representations generally gives way to enthusiasm about the 'next big thing' – one which is also starting to be taken up in schools, hospitals, worker productivity and other institutional contexts (2014).

[44] As of 2016, phones have been released, or prototyped, with accelerometers (movement and orientation); gyroscopes (angular rotation); magnetometers (metal); proximity sensors; ambient light sensors; heart rate monitors; DNA molecule detectors; air quality / gas sensors; barometers (atmospheric pressure); thermometers and more.

sensors', which typically include both sensors for input like light levels or acceleration, and microprocessors for handling signal input and algorithmic analysis before the data leaves the unit, had achieved the low power requirements, small size and affordability conducive to widespread deployment.[45] Sensors also began to exploit the wider availability of wireless connections and cloud storage for two-way communications with more powerful machines (such as the user's desktop). These real developments were understood by many contemporaries to be a long-awaited deliverance of their own technological imaginations. The boom in self-tracking was knitted into a grand narrative of the 'Internet of Things'[46] – itself a reprisal of ubiquitous computing, ambient intelligence, and other theories of smart machines dating back to the 1980s and 90s.[47] It was hailed as the tech trend

[45] Discussions in the IEEE [Institute of Electrical and Electronics Engineers] community also converge with this description – as going beyond representing the sensed phenomenon and towards the information's integration into a network (Zhang et al. 2004). This distinction between 'dumber' and smarter sensors is widespread (e.g. Spencer Jr. et al. 2004).

[46] The Internet of Things thus designates a broader set of connected objects; our analysis is limited to self-trackers, insofar as their pursuit of automaticity and intimacy drives their particular epistemic impact.

[47] Both ubiquitous computing and the Internet of Things were coined by individuals at the intersection of commerce and R&D. For the former, it was Mark Weiser at the Xerox PARC laboratory, a major R&D centre with a history of landmark contributions to commercialised computing technologies; his thoughts on 'invisible' computing also influenced experiments with wearable computing in the 80s and 90s (Ryan 2014). For the latter, Kevin Ashton had been referred by his employer, the consumer goods giant Procter & Gamble, to the MIT Media Lab to work on RFIDs. Beyond the specific terms, visions of smart networks came hand in hand with work on what would become the world wide web during the 1980s – including the famous Coke machine in the Carnegie-Mellon computer science department building, which was coded to monitor its own stock in 1982 (*Carnegie Mellon University* n.d.), and was followed up by the Internet-connected toaster in 1990. Fictional and speculative

"that will define 2014" (Frog 2014); an innovation predicted to hit big time in 2013 (Wadhwa 2013); a tech "about to go macro" (Brandon 2013), or even, one of the decade's defining innovations that will have "invented the future" (*Wired* 2013). This hype was not entirely unjustified; several billion internet-connected devices had already entered the market by 2015, and optimistic projections for growth (e.g. *Gartner* 2015; Rohling 2015; Evans 2011; see Fig.5.) were being backed by a majority of experts (e.g. Anderson & Rainie 2014).

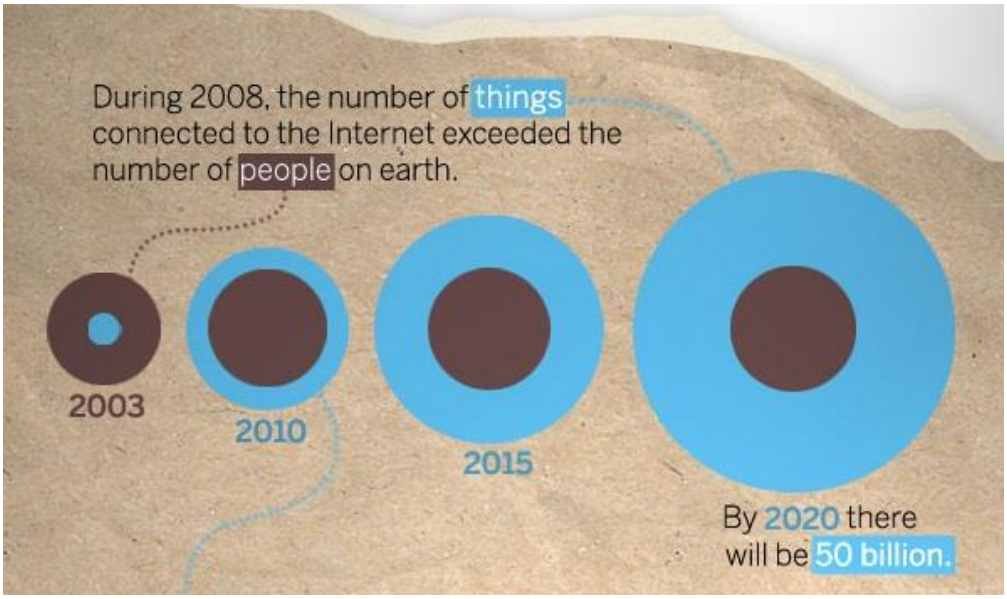


Figure 5. A CISCO Infographic in 2011.

Our analysis, then, must navigate the many intersections between deployed practices and futurist rhetoric. If the former represents empirically concrete

visions of smart homes and experimental efforts at wearable machines themselves have a history reaching back the entire 20th century.

instances of public 'uptake' of these practices, the latter were also meaningful actions that sought to organise the public understanding of self-surveillance's virtues and ideals. This chapter critically analyses the epistemic relations between 'big' data, 'smart' machines and human subjects by asking: what kind of knowledge becomes privileged as objective and accurate? Who, or what, is granted what kinds of veridical authority over the self? The object of analysis here is not the success and failure of this or that technology, but the ongoing history of what Foucault in his last works called alethurgy. "Etymologically, alethurgy would be the production of truth, the act by which truth is manifested"; not 'what truth?', but which actors and forms accrue the status of producing truth (Foucault 2011, p3). In our case, the question is how society organises the self's ability to speak its truth, to make itself intelligible. In other words, the conditions under which individuals are encouraged to know themselves, and the technological design that configures their ability to datafy themselves, structure the ways in which we make ourselves intelligible to ourselves in the first place.[48]

[48] This is what Foucault calls a regime of truth, "that which constrains individuals to these truth acts, that which defines, determines the form of these acts and establishes their conditions of effectutation and specific effects" (2014, p93). It is about the power relations and definitions of 'truth' that subjects sign up onto in order to claim 'their' truth (Velasco 2016); in other words, "every regime of truth requires the individuals who are implicated in it to engage in a specific *self-constitution*" (Lorenzini 2016).

This chapter proceeds in two broad phases. The first two sections examine dominant public presentations of self-tracking in early twenty-first century discourse. As we saw with Beddit and Thync, this discourse embraces a vision of automated and intimate surveillance, which is then promised to deliver superior control and objective knowledge over the self. Parallel to the analysis of state surveillance in Chapter 1, these sections consider what epistemic relationship, what definitions of knowledge and knowing subjects, is being presented to the public as appropriate to the new media society. The latter two sections take a more critical and historicised approach to explore alternative understandings of self-surveillance's regime of truth. Insofar as this dominant vision is merely *dominant* and never universal, we find, both amongst hardcore trackers and its most vociferous critics, a 'polytheism of scattered practices' that lurk beneath the reigning interpretation (de Certeau 1984, p48). I also address self-tracking discourse's relentless focus on the present (and the future imagined by that present). Looking back to older technologies of self-knowledge – specifically, Antique self-writing and truth-telling – can provide a schematic perspective over how twenty-first century self-tracking departs significantly from earlier efforts to 'know thyself'.

DATA'S INTIMACY

> "Self-knowledge through numbers."
> -The slogan of quantifiedself.com (*Quantified Self* n.d.)

Yaroslav Faybishenko, a portfolio manager based in New York, was driving when his wife asked the most mundane of questions: had the baby wet herself? But that was when he realised "she was sitting in data" – data that could, should, and would be mined. Only a rigorous quantification of such data could produce objective insight, he thought; and only automated, machinic tracking could achieve such rigour (Hardy 2013). Such stories of 'awakening', and the resulting hyperattentivity towards previously hidden aspects of the self, is littered throughout self-tracking discourse. This intersection of the personal and the objective was expressed through three interrelated narratives about the virtues of self-tracking. These promised virtues consisted of: (1) an unprecedented and empowering individualisation of knowledge, in part overcoming and in part supplementing the population as a unit of analysis; (2) an ubiquitous tracking environment that can capture the self and deliver objective and comprehensive self-knowledge largely independent from human guidance or awareness; (3) a democratised ownership of personal data that is currently being exploited by states and corporations. These narratives combined to promote a 'healthy' skepticism of

human intuition and experience, and a corresponding faith in machinic senses, in some of the most internal, private realms of the 'self'.

First, the advent of self-tracking was positioned as an individualising upgrade to the *population* as a unit of analysis and knowledge. The concept of population had developed in the 18th century as an effort to 'know' a human multitude that was threatening to grow beyond traditional means of approximation, especially lived intuition (e.g. Foucault 2004; Ruppert 2011). The data it provided for the 'end user' allowed the individual to compare him/herself to their proper category, or even to approximate one's individual value when it could not be directly measured. In my fieldwork, many QSers framed their own motivation to self-track as arising from frustrations with this populational, averaging calculus.[49] If people seem to respond to caffeine or cardio exercises in different ways, how can I figure out what 'works' for me? The idea was that self-tracking could answer, in ways that traditional, limited-sample populations could not (or could only roughly predict), how *I*

[49] Such efforts echoed the backlash against statistical determinism as early as the 1840s – when, perceiving a similar 'love of numbers' across contemporary analyses, contemporaries complained that such knowledge could not answer the question of what will happen to *me* and what *I* must do now to better my chances (Hacking 1990, p145). That said, self-tracking does not sit opposite populational data, and often seeks to work together – e.g. using its personalised surveillance to build up a database of the 'Quantified Us' (e.g. Jordan & Pfarr 2014).

personally would fare (e.g. Zemrani 2015). QSers frequently contrasted their solutions with a lifehacking technology of a previous generation: self-help and do-it-yourself books. They argued that whereas such techniques might insist on a one-size-fits all solution applied to a generalised cohort, QS would help you discover what protein shakes or fish oil is really doing in your specific, individual case (e.g. Swan 2013, p92; Wolf 2010b). The recurring insistence on a unique, individualised data point thus marks the promise of a particularly self-oriented (or, in the eyes of some commentators, 'narcissistic' (e.g. Bhatt 2011; Hesse 2008; Morga 2011)) knowledge. If Alphonse Quetelet had devised the average man, *l'homme moyen*, two centuries ago as an ideal fiction to understand each individual by, self-tracking practices endeavour to produce an individual without the spectre of that average – or, at least, produce an individual who is averaged within him/herself.

This vision of individualisation through machines that delve deeply and precisely into the self was most pronounced in health and well-being tracking. Beddit, as we saw, offered an ability to persistently track sleep patterns in the individual's natural habitat – something that existing clinical devices like polysomnograms could not offer. Devices designed for individual, consumer-level use grew in tandem with so-called 'mHealth' or

'e-Health' devices that would allow everyday self-tracking to communicate personal data to hospitals and healthcare practitioners. Sano Intelligence's skin patches monitor the subject's bloodstream for glucose and potassium levels, and automatically alerts his/her doctor if dangerous levels are reached; skin tattoos (mc10), wearable bandages (BodyGuardian) and biodegradeable, ingestible pills (Proteus) similarly began to extend the capacity for comprehensive, individualised data to the health and medicine industries. Here, self-tracking was seen to offer data "more 'objective' than the signs offered by the 'real', fleshly body and patients' own accounts" (Lupton 2013a, p398). The importance of such knowledge was asserted on the basis that you *need* to know to have a 'good' – fitter, happier, more productive, more confident, self-aware, less stressed – life (also see Crawford et al. 2015; Lupton 2012).

Crucially, new technical capacities for persistent, automatic, proximity measurement also opened up kinds of data that were previously not subject to mass surveillance, from subjective ratings of mood to the exact size of each person's social network (e.g. Mallett 2014). Where tracking technologies colonised new aspects of the human self for surveillance, its proponents consistently argued for the superiority of machinic accuracy and objectivity

over the educated 'guessing' of human subjects. Thus a vision of individualisation and 'patient power' intersected with a prioritisation of machinic senses over the human, albeit in a partial and specific sense (e.g. Swan 2012). If the key process in state and corporate surveillance is to extract highly individualised information for each and every person, self-tracking also seeks unprecedented frequency, immediacy and accuracy through its 'personalised' observation. In Quetelet's time, statistical norms and populational data evolved quickly from a method of approximation to a production line for ideal norms and 'average men' (see Hacking 1990). Today, self-surveillance contributes to a wider trend that has been called an 'unofficial resurgence' of logical positivism (Lanier 2010, p155): a renewed confidence in the power of new, 'big data' technologies to deliver truth more objective than ever.

Figure 6. The 'universal monitoring solution'.

Second, self-tracking technologies increasingly turned towards an environmental and atmospheric form of everyday presence: a *background*. They were designed to become 'part of the furniture', rather than standing out as discrete and actively used tools, spatially bound archives, or specific and purposeful queries.[50] By the early 2010s, devices were beginning to accompany users to the bed and the bathroom; in their walks up the stairs as well as runs in the park; in their phones and even, as we have seen, under their skin. Previously, measurement and its archival had typically been confined to specific and comparatively stable classes of objects and situations; the bathroom weight scale, the diary or journal, the doctor's office, the desktop computer. The shift towards ubiquitous sensors and prosthetic devices entails a qualitatively distinct relation of surveillance. Consider 'Mother'. (Fig.6) This product offers small, nondescript 'motion cookies' that can be attached to domestic objects like toothbrushes and pill-boxes. The cookies' motion, temperature and proximity sensors allow continuous monitoring of whether the keys have been picked up, or the front door has been opened. While each given implementation is rather nonspectacular, such

[50] This kind of design objective was strongly influenced by commercial interests; industry actors commonly spoke of the importance of achieving 'low maintenance', 'frictionless' surveillance to win over the wider public to self-tracking practices (e.g. Holland 2013; Reeves 2015). In another sense, the idea of background is closely tied to what we will describe as machinic sensibility: the production of 'self'-knowledge by undercutting and bypassing human attention and activity.

tools point towards a domestic environment where tracking passes from a *specific action* to a general fact (also see Rettberg 2014): as one industry insider put it, a 'planet with a nervous system' (Hernandez 2012).

Such environments extend the well-documented, Internet-age tendency towards a phenomenology of distraction and abundance (see Thrift 2011; Berry 2011; Wajcman & Rose 2011). By building a complexity of automated observations and communications across various sensors, the human user is positioned not as a centralised controller over each process but a responsive actor that is alerted, interrupted and otherwise 'lead on' by this 'smart' environment. No doubt each user, and each use situation, then develops its own conventions; some users will frequently exercise their sovereign right to override the analysis and recommendations, others will be habituated into their guidance, and yet others will simply ignore them. Yet in all cases, the design behind these implementations carry with them a set of epistemic affordances that cannot be ignored. Take another example – this time, one that is still slightly ahead of the curve of popular uptake, but still utilises technologies already being deployed across American homes in less

comprehensive ways. Tahl Milburn is a QS enthusiast[51] who has designed and installed what he calls a 'Life Automation System' [LIAM] in his own home (Milburn 2015). There, USB sticks and other objects glow ambiently with a variety of colours – colours which correspond to a single 'LifeScore' derived from personally tailored and weighted variables. The score considers Milburn's net worth; the market performance of his investments; weight; activity; sleep; age; and more. The colours thus act as a persistent, if backgrounded, reminder that he has 29 years of life remaining (estimated), or that his net worth has risen. In a similar vein, Ariel Garten – who appeared briefly in the Introduction in her involvement with Muse, the brain-tracking headband – put it to me terms of a "practice of noticing"; a machinic habituation of human attention that would cultivate the desired (in this case, productively focused) consciousness to begin with (2015, personal communication). Thus, such an environment is designed to make subjects *forget* their own condition of self-surveillance. In my fieldwork with QSers, many described their longer-term experience with tracking in similar terms; an experience where data, and its influence upon one's habits, decisions and

[51] Milburn is another example of the intersections between QS and the self-tracking industry, between personal and commercial interests. Having worked in consulting and management with internet technology companies, his experiments with LIAM – deliberately or emergently – led to a startup that was, as of writing, seeking to develop the system into business-targeted products.

interpretations, becomes backgrounded and 'forgotten'. By the early 2010s, we find the commonly vocalised sentiment that self-tracking needs to improve its ability to hide in plain sight – easy to use, unobtrusive, hardly noticeable in most cases – to achieve truly widespread appeal (e.g. Hardy 2013; Swan 2013, p88; Watson 2013b; Weintraub 2013). Even as self-knowledge becomes more comprehensive and ubiquitous than ever, it also withdraws into the background and out of subjects' conscious engagement.

Finally, the individualisation of data was heavily connected to hopes for empowerment and *ownership* for self-trackers. It was not uncommon for QSers and self-trackers to position themselves as analogous to Stewart Brand and the countercultural influence upon computing between the 1960s and 1990s (Turner 1996; also see Sharon 2016). Just as those 'hippies' took a military-industrial technology and helped produce a culture of personal computers and 'digital utopianism', self-trackers would act as vanguards for turning the tide of data towards empowerment and democratisation: personal computing 'all the way in' to the self (see Watson 2013a, p11). In 2011, at the very first Quantified Self conference, Gary Wolf introduced the movement in these very terms:

> We saw a parallel to the way computers, originally developed to serve military and corporate requirements, became a tool of communication. Could something similar happen with personal data? We hoped so (Wolf 2011).

In this vein, it was argued that self-tracking could become a way to take 'back' our data that states and corporations have been using against us.

> …why shouldn't you have access to the traces of your own behavior that you leave behind and that others collect? […] 'It's more of a cultural shift,' she says. 'It's about creating a culture where we own this data. This data is ours.' (Walker 2010)

Such sentiments were shared across a broad coalition of actors, from QSers to journalists and user testimonials. One entrepreneur, whose company provides microbiome analysis services for individuals, depicted a trajectory whereby the individual was formerly left at the 'periphery' of the traditional health process, crowded out by experts: now, "I test things on myself, I know what is happening, I am not the body that the scientific and medical establishment acts upon" (Brouwer et al., 2015). Laurie Frick, an engineer-turned-artist who promises "a glimpse into a future of data about you" (Frick n.d.), vocalises a rather pragmatic attitude: "I think people are at a point where they are sick of worrying about who is or isn't tracking their data […] I say, run toward the data. Take your data back and turn it into something meaningful" (Urist 2015)

– in her case, personal data diagrammed into art. It's *your* data, many self-trackers insisted, so surely you should get as much use out of it as the others do.[52]

Indeed, self-tracking's narrative of ownership was framed in terms of wider public debates around the exploitation of personal data. Most individuals sufficiently interested in their own data to attend QS meetings, or even simply purchase ready-made devices like the Fitbit, would have been keenly aware of contemporaneous controversies regarding not only the Snowden Affair and state surveillance, but corporate data-mining. By the 2010s, increasingly sophisticated techniques for extraction and analysis of online communications data had intersected with a thriving advertising market, leading to fears of a 'personalised' web and automatised, algorithm-driven discrimination of customers at a mass scale (e.g. Turow 2011; Cheney-Lippold 2011; Pasquale 2015b). With all this as background, self-tracking enthusiasts often argued that if everybody is going to measure us anyway, we might as well accept the situation and make the best of it (e.g. Finley 2013; Havens 2014, p53). The

[52] Contemporaneously, similar sentiments were being expressed in other sites of data exploitation. Some musicians have argued that they should actively take 'ownership' of their data – which, in practice, means collaborating with corporate data-mining, and then finding ways to leverage that information to optimise their own strategies for monetisation (e.g. Meyer 2012).

rhetoric of individualised control thus left the problem of privacy on the periphery, even though self-tracking was already harvesting, and sometimes sharing, the kinds of data that corporate surveillance at the time could only dream of having.

All in all, the dominant presentation of self-tracking – the practices and their interpretations offered to the public at large – intersected and conflated personalisation with objective truth and individual control. At the same time, we find the valorisation of a machinic environment that surrounds, bypasses, and structures *a priori* the very conditions of the subject's experience of self-knowledge and self-improvement. Key elements of Mark Hansen's twenty-first century media (2015), which we had identified in state surveillance, and the basic principles of recessive epistemic relations, thus co-habit a practice invested in the idea of a more rational, more independent, more knowledgeable human subject. This hybridisation is exemplified in the words of Ariel Garten:

> My goal, quite simply, is to help people become more in tune with themselves. I take it from this little dictum, 'Know thyself.' If you think about it, this imperative is kind of the defining characteristic of our species, isn't it? […] I'm here today to share a new way that we're working with technology to this end to get familiar with our inner

> self like never before - humanising technology and furthering that age-old quest of ours to more fully know the self (Garten 2011).

There is an odd, more or less posthumanist sentiment here: good old humans need some technology to become fully human, or at least, a better kind of human. Within this perspective, the clichéd refrain of our age – 'Just be yourself' – no longer holds out an emancipatory vision of a sovereign individual unfettered by conformist norms, but a troubling epistemological problem: do *I* have the capacity to know what I 'really' want? Enthusiasts insist that self-tracking is about 'planned serendipity': when you surrender yourself to machinic collection, the data should be able to come back and surprise you about questions and patterns you had never even considered (Sterling 2013).[53] Just as the NSA argue that you cannot filter anyone out because you don't know what a suspect looks like until you see it, self-tracking reserves a certain proactive role for data and algorithmic analysis. We will examine this tension more closely in the next section. How does self-tracking's vision of conquering new uncertainties, its belief in the virtuous

[53] Like many other aspects of self-tracking, this vision of planned serendipity was shared across projections in Internet, Internet of Things and other data-driven technologies. Google, having made its name on faster and better search, envisions search to become so efficient it jumps ahead of the querying human; in 2010, Google co-founder Eric Schmidt made headlines with the claim that Google's future is to tell people what to do (Jenkins Jr. 2010). It was received as marvellous, creepy, or both. The claim turned out to have a rather fast turn-around into concrete technologies. The next few years saw predictive reasoning assistants like Ciri (Apple, 2011), Google Now (2012) and Cortana (Microsoft, 2014) enter, and assimilate, into Western societies.

coupling of computational automaticity and objective truth, position the subjects themselves vis-à-vis the epistemic process? What are the consequences of the increased responsibility and automaticity granted the machine upon the relation between the subject and his/her own 'self'?

DATA'S PRIVILEGE

> 'For a certain type of person,' says Wolf, the Quantified Self founder, 'data is the most important thing you can trust. Certain people think a feeling of inner certainty is misleading.' […] Computers don't lie. People lie (Hesse 2008).

People lie – about themselves, and especially to themselves. One dominant trope regularly wheeled out by both enthusiasts and skeptics (and those in between) is that self-tracking heralds an environment where *you cannot lie to yourself* anymore. We may knowingly tell fibs to ourselves about eating too much and running too little; we may not even notice that the eight-hour work day just included three hours of web-surfing. But the data will not filter out your momentary indiscretions, your corner-cutting, and it certainly will not parlay with your pitiful excuses. Human memory, consciousness, reason, so often is a cursed fog upon clear sight; data, unforgiving and unyielding, will scatter the confusion. Or at least, that's the idea. As Gary Wolf puts it elsewhere:

> Can our devices know us better than we know ourselves? It seems obvious that this must be true. Human self knowledge is plagued by all kinds of limits: bias, sampling error, memory failure, and lack of sufficient processing power to recognize complex patterns (Wolf 2008).
>
> I suspect we are in no position to stand guard over our judgments without the help of machines to keep us steady (Wolf 2009a).

The language of trust, lies and self-rationalisation carry certain implications about the affects and experiences entailed by a self-tracking life. Here, however, our focus is strictly on the epistemic relation between subjects and self, mediated by machines and data. To speak of such relations systematically, we must differentiate between the experiencing, reflecting, conscious 'I' – which we have typically referred to as the subject – and the physiological, behavioural, neural, affective, and otherwise empirical 'me' or 'self'. In self-tracking discourse and its articulation of 'lying to myself', there is an epistemic gap between the I and the me; a gap which ensures that the me is a perennial source of uncertainty and unknowability for the I. In this narrative, the pre-tracking subject is one which regularly forgets, is confused, rationalises, narrativises, and yes, 'lies' to oneself. In contrast, self-tracking technologies can then offer an externalised and objective other – one which is able to intervene very particularly upon the subject's claim to his/her 'own' truth. In that sense, self-tracking is quite literally a self-surveillance. When the

subject consults tracking data and its recommendations, and that data is socially invested with a certain value in objectivity and accuracy, the encounter between the I and me becomes an occasion where my self-knowing is *tested* by the epistemological framework of the tracking machine.[54] To assess whether I have been diligent today, I must determine the standard by which diligence is defined; the facts of my actions on that day; any extenuating factors; and how they are all to be calculated towards the standard. Self-tracking seeks to break up and externalise these various micro- or partial judgments, calling upon the I to consult and negotiate the machine and its reports to arrive at the final call (including a successful act of 'lying to myself').[55]

Such a mediated relationship extends and qualitatively transforms the epistemic processes found in pre-digital forms of self-tracking. When Benjamin Franklin (1884) daily recorded his observance of thirteen virtues (Fig.7), it was a discrete and ritualised process presided over by the reflexive subject. Franklin had devised a simple database, whose catalogue of

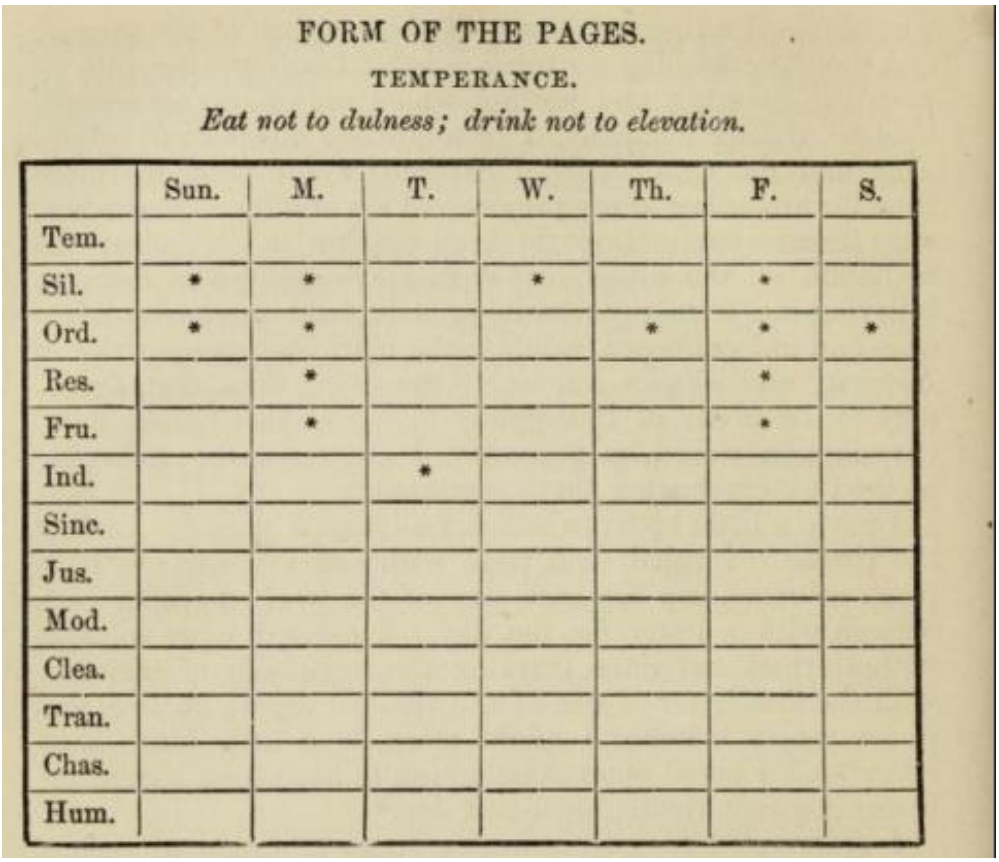
[54] For a longer history of such overcoding, see Theodore Porter (1995)'s analysis on quantification as a 'social technology' which produced new valuations of precision and efficiency with practical consequences for the fields it touched, like barometry and cartography.

[55] A roughly analogous use of 'test' may be found in (Boltanski & Chiapello 2007).

predetermined categories of virtue would ask: had he been temperate, had he been chaste? And he would record 'a spot' for each transgressive day. In other words, Franklin's own interpretive faculty was central to data curation. Arrangements like Beddit, Mother, or LIAM make a clear departure from this relationship. Consider RescueTime – a web browser extension that monitors computer use, a relatively simple kind of tracker. It silently fills a record of distraction, procrastination, and that elusive 'true productivity', in ways that few humans would be able to accurately recall on their own. Do you tend to slack off more often on Wednesdays? Do you spend 24% of your desk time on social media? While all kinds of holistic reasons would have entered into such behaviour, it is the beauty and terror of correlational epistemology that it will produce conclusions purely based on what it measures, and in doing so, suggest that what it cannot measure pales in comparison to the correlation it *can* calculate.[56] In this new breed of self-trackers, more and more of the knowledge production process occurs beyond the subject's experiential access – such that the machines, the categories, the databases, extract relevant data directly from the empirical self.

---

[56] An analogous development can be found in the history of the intelligence quotient [IQ]. Its inventor, Alfred Binet, explicitly specified that his tests could not properly represent 'intelligence'. The tests were instead designed to provide an internal consistency and comparability, such that if a child scored lower across ten or twenty tests, he or she could be identified as in need of special education. Thus Binet wrote, "It matters very little what the tests are so long as they are numerous." (1911, p329 *in* Gould 1996, p179)



FORM OF THE PAGES.

TEMPERANCE.

Eat not to dulness; drink not to elevation.

	Sun.	M.	T.	W.	Th.	F.	S.
Tem.							
Sil.	*	*		*		*	
Ord.	*	*			*	*	*
Res.		*				*	
Fru.		*				*	
Ind.			*				
Sinc.							
Jus.							
Mod.							
Clea.							
Tran.							
Chas.							
Hum.							

Figure 7. Franklin's table of virtues.

As mentioned in the previous section, this difference, this 'bypassing', aligns closely with Mark Hansen's notion of twenty-first century media (2015). Using his language, we might call this communication between machines and the empirical self, the communication which at least initially bypasses the conscious subject, as *machinic sensibility*: self-tracking technologies' capacity to observe and collect data in ways that human sensibility cannot reach, and sometimes, collect the *kind* of data that humans cannot reach (also see Swan

2012, p235). Some measurements, like galvanic skin response[57], are absolutely beyond human access; others, like steps taken, are measured with a frequency and precision practically unavailable to human subjects. The result is formally analogous to the effect of 'black-boxed' algorithms in social media platforms and state surveillance systems (e.g. Amoore 2011; Bucher 2012; Gillespie et al. 2016; Pasquale 2015b): the many micro-judgments that go into what counts as a step, what counts as 'good' sleep, what counts as 'excitement' are increasingly placed outside the subject's reach. The result is a powerful filter on what 'counts' as relevant towards self-knowledge, and *how* it is counted.

In short, there was a certain investment of veridical authority upon tracking machines, one which prioritises machinic sensibility as the privileged route to objective self-knowledge. Yet this is not simply a zero-sum game where the subject finds him/herself alienated and powerless. Subjects are never guaranteed to accept that machinic authority straightforwardly, and even if they do, it is not necessarily at their 'expense'. It may be more appropriate to say that self-tracking encourages its practitioners to step back and develop a certain skepticism about the I's intuitive, experiential access to the me – and,

[57] In most cases, human subjects are incapable of sensing, or consciously controlling in any direct fashion, their electrodermal activity.

in turn, legitimise machine-sensed data as something that more adequately *represents* the self. During the early 2010s, the stakes of such rebalancing in knowledge production remained ambiguous, largely because the technology was first and foremost understood in instrumental terms: as tools that let humans do what they want to do. Yet the recent history of corporate surveillance, which had matured well before self-tracking, indicates the broader structural effects of these 'mere tools'. Over the 2000s and 2010s – what came to be known as the 'Web 2.0' era – it was the very promise of empowerment through online connectedness that coaxed billions of users to *voluntarily* opt into the relentless surveillance and exploitation of their own personal data. The convenience of 'connectedness' had as its price a 'connectivity' to vast corporate surveillance systems (van Dijck 2013), and users only belatedly realised that "if you're not paying for it […] you're the product being sold" (Oboler et al. 2012). In the same way, self-tracking is beginning to coalesce into a wider ecosystem, interlinked webs of significance, whereby machinic sensibility's primacy over human sensibility might be formalised at social and individual levels. In 2014, the popular fitness tracker Fitbit was called as a legal witness; a Canadian law firm invoked the client's own tracking data to prove that a work injury had affected her physical activity levels adversely (Olson 2014). Although the data

was here summoned by the 'I' (or, the I's legal representatives) to support its self-narrative, such cases look forward to a near future where the datafied 'me' could appear in court, and establish an authority over the truth of the self that can override the subject's own words and memories.

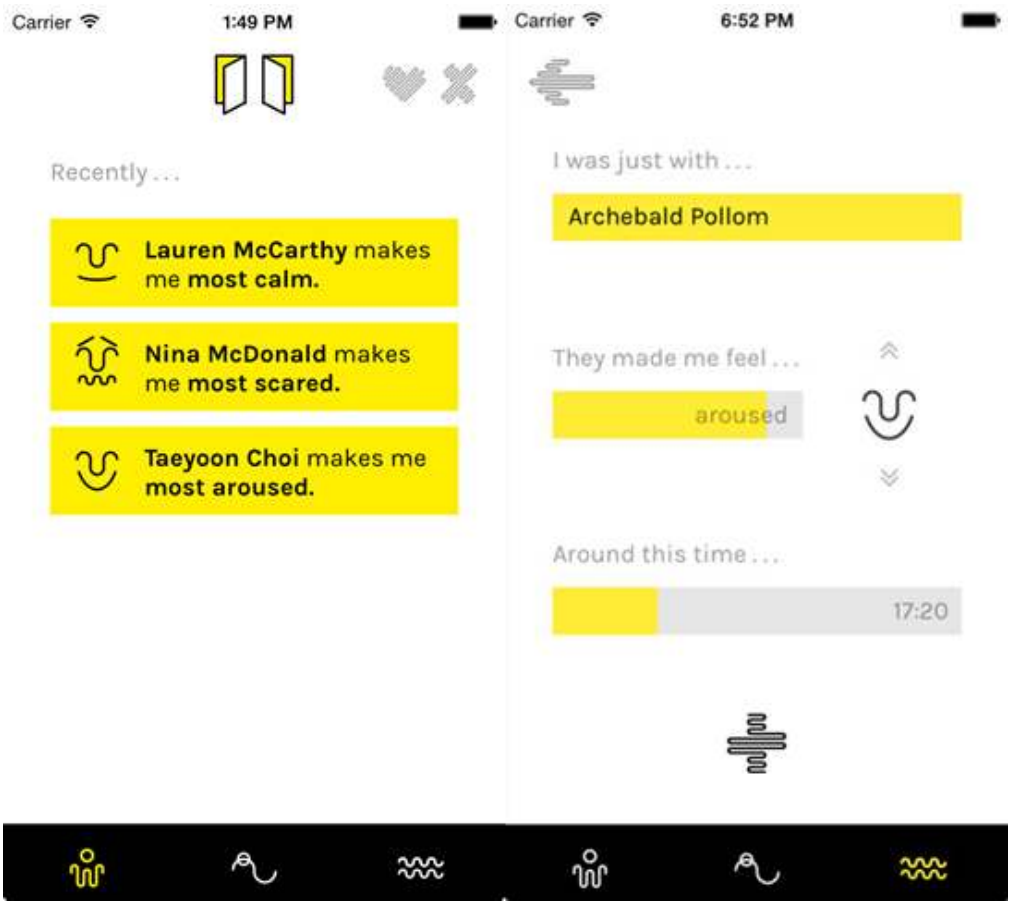


Figure 8. The pplkpr interface.

Tellingly, such a redistribution of veridical authority tended to elicit critical responses when they encroached on aspects of everyday life that traditionally were considered too private, too subjective, too emotional, and otherwise too

sensitive to measure and clarify. pplkpr is an app which leverages smartphones' ability to collect heart rate variability and locational data, and combines it with users' manual input of who they were meeting and how they feel. The data is used to deliver correlations about which acquaintances might make the user more nervous, more aroused, sad, happy. (Fig.8) As the promotional trailer says:

> See how your relations stack up, and let pplkpr find the ones that work for you. It'll automatically manage your relationships so that you don't have to, scheduling time with people that make you feel good, and blocking the ones that don't. Forget fake friends, failed romance, and FOMO [Fear of missing out]. Optimise your social life with pplkpr (*pplkpr.com* n.d.).

pplkpr presents user testimonies that point to the kind of veridical authority commanded by data's claim to objectivity. "Using the app as a justification for not wanting to spend time with someone is a lot more definitive than just saying, I'm uncomfortable", says one; "It made me realise the truth," another. pplkpr, in fact, was created by two Carnegie Mellon artists-in-residence, who appeared happy to leave the app's status ambiguously between a genuine belief in 'optimising social life' and a provocative lampooning of it (e.g. Beres 2015). Much more earnest – and controversial – was Peeple, an app which was announced in late 2015 promising a fully public system for quantitatively

rating ordinary humans. Individuals would be broken down into romantic, professional and personal 'scores' as rated by their acquaintances – and they would not be able to opt out. Peeple, strictly speaking, is not a self-tracking app; lying on a continuum that includes pplkpr and other more self-oriented practices, however, it is an important case study in how quantified knowledge of the self can start to 'count' in social and institutional contexts. Once brought to public notice through *The Washington Post*'s coverage (Dewey 2015), Peeple set off a firestorm of international controversy; the soon-to-come app was quickly branded a "creepy" poster child for the dangerous implication of a 'rating' society (Chamorro-Premuzic 2015; *BBC News* 2015) where humans are reduced to singular numbers (Pasquale 2015a). It would ultimately launch a few months later, though at time of writing, its eventual impact – whether as a case study in the steady march of trackers, or their backlash – remains in the air.

From the refrain 'you cannot lie to yourself', to data that speaks for the subject in the court of law, to a data-driven audit of one's friends and acquaintances, the hopes and fears surrounding tracking technologies are closely connected to the epistemic power invested in the process of quantification and datafication. If self-tracking technologies promise accuracy and objectivity in

all things about the 'me', the corollary is that it threatens to deprive subjects of traditionally tolerated margins of transgression, the epistemic 'spaces', the *uncertainty* that allow for subjective self-determination. In Chapter 1, we mentioned Žižek's counter-argument on Foucaultian discipline: is not discipline, and its external order, a means by which individuals gain "precious space in which to exercise [their] freedom" (n.d.)? Now, we must return yet again to discipline's more orthodox function: self-tracking's promise of certain knowledge, insofar as it becomes socially legitimated, threatens the many ways in which subjects' perception of themselves depends on what is left ambiguous, implicit, uncertain.[58]

***

The privileging of machinic sensibility over such uncertainty is especially significant because many self-tracking technologies of this period were conceptualised as tools not only for observation and prediction, but recommendation, curation, nudging, habituation. This trajectory is well summarised by Vinod Khosla, a tech industry veteran who had co-founded

[58] This is another take on Lauren Berlant's point that subjects are often well versed in managing affective incoherence and disorganisation, defending their own contradictions in their own terms (Berlant & Edelman 2014, p6; Berlant & Greenwald 2012).

Sun Microsystems in the 1980s and is now a key figure in the QS and self-tracking industry. "Humans look for what they know to look for. The next generation of algorithms will look for everything", Khosla (2015) exclaims – and then tell us what we didn't know to look for, to boot. And such a vision, both idealistic and commercially compelling, directs funding; Khosla's own venture capital firm has invested millions into tracking technologies like blood pressure monitoring (Quanttus), sleep monitoring (Misfit), fitness tracking (Jawbone) and general health behaviour tracking through smartphones (Ginger.io). Other actors in the tracking business similarly speak of using tracking to "change the way we feel" (Siegel 2015)", a 'planned serendipity' (Sterling 2013) where the machinic system furnishes the moment you are to seize (Havens 2014, p58-9).

Nudging – which can include recommendations, reminders, encouragements, guilt-trips – is a familiar term within self-tracking discourse. Writing in the *Harvard Business Review*, one high-ranking consultant (Wilson 2012) offered a classification of two types of self-tracking: trackers and nudgers. But already, there is no clean split: a tracker "reveal[s] patterns and help[s] you set goals" by virtue of its measurements. As soon as the machines produce systematic, longitudinal data and present them to the users, there is more than 'just

counting' going on. When nudgers are described as "guid[ing] you toward your goals by asking questions or prompting action on the basis of the data they've received", this is something that applies to self-tracking as a whole. Moov NOW, branded as a 'personal coach and workout tracker', combines sensor-based tracking with a talking personal assistant in the user's ear, one which provides real-time encouragements and instructions:

> The personal trainer aspect of the Moov NOW is extremely active and engaging, constantly pushing you to go further and improve your form. I was fairly blown away with how specific an instruction it was capable of giving; at some points [it] would tell me to 'land softer on my feet' or 'unclench my fists' while jogging (Lauletta 2016).

Even without tapping into the popular imagination of speaking artificial intelligence, the organisation and presentation of tracking activity itself plays a nudging role. Basis Watch, which features sensors for heart rate, daily steps taken, calories burnt, sleep type (deep vs. REM), and a record of daily activities, insists on calling its phone app 'Habits'. Habits is a dashboard which asks you to set goals for, say, sleeping earlier, or walking more.

> In the beginning, you can only sign up for three habits, but over time, as you consistently practice good habits, you earn the right to add more. Between that and the encouraging green color-coding, I feel like

> I'm being rewarded for good behaviour, and I feel motivated to keep up my winning streak (Wollman 2014).

To be sure, such blatant Pavlovian conditioning can hardly be assumed to be a universal response. Each device will play host to a variety of emergent and transgressive uses, twisting the data and functions into unintended roles. Yet the ways in which these technologies are designed, presented, packaged into rhetorical gloss, organises the kinds of affordances they communicate. And insofar as they act automatically to recommend and 'nudge', self-trackers increasingly organise the epistemic situations into which subjects are positioned, even if their responses will vary.

Facing what it believed was a new evolution of terrorist threat, the American state turned to indiscriminate, automated, machine-driven surveillance, in the belief that data's objectivity and rigour would achieve the kinds of knowledge and certainty humans were not capable of. Only a few years late to the party, self-trackers are also hoping to bypass the thinking, feeling subject in order to arrive at the objective truth of what the self is and what is good for the self. In this schema, the I, and its subjective faculties of knowledge, become thoroughly distinguished from the objective me; and the machines, with their

privileged access to the latter, are increasingly designed to *lead* the subject in the auto-analytic, auto-epistemic process.

> I talk about the dopplegänger principle because I feel like every single person has a life that they believe that they lead, and then they have the reality track. The reality track is what we do, the data track. For most people, those only overlap by about 60, 65% (Mette Dyhrberg, 2015, personal communication).

DATA SKEPTICISM

Let us recount our steps. Self-tracking technologies promise one more victory, one more historical advance, in the long war against uncertainties and unknowns that plague self-knowledge and human intuition. At the same time, such a promise depends on the deployment of autonomously observant machines on our bodies and in our everyday environments. This tension between the promise of knowledge and the privileging of data epistemology did not pass unnoticed – although it was rarely expressed in schematic terms. Not everyone shared in the dominant rhetoric of self-tracking's virtues and benefits. Self-tracking's popularisation prompted backlashes in the public sphere, a decentralised set of sceptics that typically questioned machinic sensibility's pernicious influence on our 'humanity'. Meanwhile, self-tracking connoisseurs in the Quantified Self community often developed a varied and evolving set of attitudes about what kinds of epistemic work they were

performing on themselves. Where the dominant rhetoric offers a monolithic and universalist vision of technological progress, these alternative attitudes reveal a certain practical flexibility and ideological *bricolage*. In this section, we focus on how the latter brings out the tension between knowledge and uncertainty in the form of a struggle between machinic sensibility and human experience.

The proliferation of self-tracking technologies from the late 2000s onwards attracted 'mainstream' media coverage beyond tech-savvy circles – and, as it did so, a distributed but consistent pattern of backlash or scepticism. The sceptics tended to rehash old binaries between nature and technology, the human and the machine, making familiar appeals to the 'naturally' human. In a typical example, the sex life tracker and gamifier Spreadsheets provoked the question, 'can the Quantified Self go too far?'

> As beneficial as a trove of personal data can be, though, there are some things better left uncharted. Comparing our friend counts and vacations with others on Facebook is already making us sad. And it's unlikely that comparing our lovers' average duration and decibel volume to others' is going to make us happy. Analytics are creeping into the most intimate and unquantifiable parts of our lives. […] "You can't substitute gamification for those core things people strive for," social psychologist and CEO of mental health network Psych Central John Grohol recently told The Atlantic. "Filling up a love tank isn't the same as having a personal connection." (Kessler 2013)

Such rhetoric presumes a common sense, a set of shared intuitions about what is 'natural' to humanity. Notably, such arguments were often grounded entirely on what they left unsaid and unspecified. How is this 'personal connection' incompatible with analytics? What makes sex 'unquantifiable', exactly?[59] The public, external criticism of self-surveillance tended to romanticise a natural human way of being. In criticising self-tracking's promises as fantastic ideals of optimised, posthuman cyborgs, they themselves tended to reify the figure of the pre-technical human and their 'natural' relationship to themselves. Such romanticism was also frequently joined by doubts and criticisms about self-tracking's efficacy. Narratives of technological optimism rarely consider the many ways in which technologies fail to be useful, or simply to function properly; when they do, such problems are dismissed as temporary roadblocks in the drama of progress. Yet self-tracking technologies available in the early twenty-first century were still riddled with many such problems.

> But does this numerical 'self knowledge' make [Gary] Wolf healthier, happier or more effective? […] They believe the maxim that only the things that are measured can be improved. But I see a lot of measuring,

[59] If it's not sex, it's vaginas: kGoal, a crowd-funded 'Fitbit for your vagina' that tracks your pelvic muscle training, was similarly criticised as "quantifying … gone too far" (Zimmerman 2014).

> but not much improvement […] for anyone serious about health, my advice is to recycle all this 'quantified self' junk, eat real food and go outside for some serious exercise every day. Instead of relying on consumer electronics to tell you how you feel, pay attention to your own body. It will be a long time before Silicon Valley invents a set of sensors better than the ones you were born with (Elgan 2012; also see Hardaway 2013).

Such commentary cast doubt on self-tracking's efficacy by arguing that good old solutions, and the natural body, are unlikely to be beaten to the self by some fancy gadgets. There is, again, the designation of a natural relationship – one which supposedly requires no explanation, being universally understood and shared by 'serious' folk. Of course, this very binary between authentic human care and machinic artifice is a fiction; humans have always been dissatisfied with their access to themselves in all sorts of ways; hence the many efforts, electronic or otherwise, to augment self-knowledge. What is significant is not that such a schema is historically correct, but that it was the standard form in which scepticism towards self-tracking was articulated. This vague, yet moral and normative, style reflected a certain unease not only with self-tracking's rigid pursuit of quantification and precision, but the basic valorisation of certainty and surveillance *in the first place*: is it really edifying to 'know' the self in this way, and is such knowledge even 'true' to the subject? Just as the proletariat need not be versed in Marxist theory to produce a genuine articulation of his/her predicament, the sceptics' semi-

Luddite discourse is itself is symptomatic of self-tracking's destabilising influence on more traditional epistemic relations between the I and the me.

The nature of this destabilising influence came into sharpest relief in the arguments raised against numbers and quantification. Any form of quantification necessarily produces its residual; the decision of what to count and how to count it requires dividing the phenomena in question into discrete, measurable pieces – pieces that are now amenable to decontextualised circulation (Porter 1995). Criticism against self-tracking's love of numbers took up two general aspects of this problem. First, it was alleged that the focus on numerical measurement privileges that which is countable over that which is not (e.g. North 2014; Ceglowski 2015). The majority of self-tracking solutions in this period relied on finding acceptable values that can serve as a proxy of the real object. For instance, some devices derived stress levels from heart rate variability, while others simply asked for a self-reported score of more composite values like 'happiness'. To be sure, the mere use of a proxy does not disqualify the measurement; but sceptics sought to show how self-tracking's promise of data-driven certainty produces its own margins of uncertainty, its own dark regions. One example concerns the aforementioned pplkpr:

> McDonald[, a co-creator,] recalls a moment during testing where two close friends were working on a school project together. The app noticed that every time the two saw each other, their stress levels would spike. "Eventually it just blocked both of them from each other," he says. This example points to how computers view data: as numbers and patterns, not mile markers of nuanced emotions. It's also a nice reminder that for all our technological advances, there are some things people still do better (Stinson 2015)

Such arguments warned that to see like a tracker is to lose an older, looser, holistic kind of perception.[60] pplkpr's provocation also touches on the second criticism. Self-tracking technologies' quantification of the self provides discrete and manipulable correlations: I walk more, my steps count goes up. Where enthusiasts saw in this relation the golden gate to self-improvement, sceptics argued that such an interface produces a misleading sense of control: one does not become 'healthier' in the fuller sense, but does become very good at optimising their Fitbit numbers (e.g. Wallace 2010; Goetz 2013). They warned that the proliferation of data was beginning to masquerade for legitimate and reliable 'knowledge'.[61] Influential technology critic Evgeny

---

[60] A parallel process, where a data-driven way of seeing colonised a more eclectic but thereby holistic and situated system of knowing, was fundamental to modern statecraft (Scott 1998).
[61] A similar argument was being raised against the use of big data (boyd & Crawford 2012) and increasingly complex models in other knowledge spheres. As part of the society-wide inquisition into the why and how of the 2008 global financial crisis, Donald Mackenzie has shown how finance software's front-end of relatively simple and easily manipulable numbers help the human analyst *feel like* they understand and grasp the process (and that, by extension, the machine certainly must be even more infallible). (Mackenzie 2010; also see Pasquale 2015b).

Morozov (2013) also joined the fray largely on the sceptics' side. Recalling a 1987 slogan from philosopher Ivan Illich, the 'imperialism of numbers', Morozov argued that quantification gives us the easy, 'low-hanging fruit' in our quest for self-knowledge, and in doing so, steers us towards a passive solutionism: just let the machines gather, and we will eventually be better off. He thus warns that the human's fate in this regime is to be nothing more than the enforcers of algorithms' findings. The attack on quantification organised the debate surrounding self-tracking into a normative and ethical problem: what kind of self-knowledge should individuals strive towards, and how? If 'better' knowledge is not simply a synonym of technological efficiency or precision, how should it be defined? If the veridical authority of the thinking subject should be protected in some way in the age of machinic sensibility, how – and why – should it be done?

These critiques were developed with greater nuance and variety within trackers, enthusiasts, entrepreneurs and visionaries. This should not surprise us; as I described in the Introduction, 'self-tracking' refers to a constellation of practices and concerns sharing key resemblances, rather than a single community defined by dogmatic allegiance. This is particularly the case with the Quantified Self community. Where its early years were dominated by an

embrace of quantification and a relentless quest to datafy different aspects of human life, it has since grown into a large, international, and yet decentralised group – one where journalists, academics, tech entrepreneurs, health industry workers, college students, and other kinds of identities intersect (also see Butterfield 2012). This has resulted in a more diverse (though still very much middle-upper class and tech-savvy) ecosystem of attitudes, one which increasingly accommodates non-quantitative practices, intersections with meditation and other spiritual techniques, and indeed a degree of scepticism about the consequences of tracking (see Lupton 2015; Lupton pre-print). QS thus includes not only those who are looking for *more* data, but those who have strong opinions about how the self *should* be analysed, and are loathe to leave those decisions for others to make.[62] In my fieldwork, many QSers openly admitted that the human is not composed of a discrete set of switches and sliders you can simply 'discover' through tracking. Rather, they tended to justify self-tracking by pointing to the kinds of attitudes, the perspectives, that the reflective I can gain by way of engaging

[62] Consistent with self-tracking's promise of personalisation, QSers tend to be cautious, or even downright critical, of conventional and/or universalising definitions. One panel at their 2015 conference began with the joke that there's a standard American diet, and a standard American doctor – the 'SADs' (Abramson 2015). (The joke was well received.) Outlandish wearables, new and weird personal habits, and other kinds of non-normative behaviour tend to be appreciated as worthy efforts to find such personal and unexpected answers to better living.

in tracking as an activity. At the 2013 QS Conference, Nancy Dougherty, a long-time tracker, discussed becoming ill, and discovering that the good old doctor, antibiotics and exercise were helping her health far more than her years of tracking:

> [When we track our health and our body,] there're so many variables with inputs we're not quite sure what to care about […] a lot of responses are time-delayed, they're interdependent, they're not linear, it's a really awful system to actually try and characterise […] I'm really really bad at understanding what's going on with me, physically and emotionally, yeah, I'm never quite sure if I'm tired, and fatigued, or if I'm just bored, maybe, or if I'm feeling good, maybe because I've modified my diet, or maybe just the weather changed… (Dougherty 2013)

Yet these thoughts did not lead Dougherty not to disavow tracking. Rather, she describes a transitional process by which she would stop tracking while holding on to a 'QS mindset'[63]:

> The Quantified Self isn't really about quantifying to me anymore […while recovering from illness,] I wasn't keeping track of anything, I wasn't logging anything, but it still felt very much like a QS experiment to me […] because I had the Quantified Self mindset. The flexibility, exploration, even just the idea that I was in control of my health, and it wasn't just antibiotics.

[63] In my research – especially in offline gatherings in New York and San Francisco, and online discourse – the language of mindfulness was commonly mobilised to talk and think about self-tracking, and QSers frequently reported using techniques like meditation in tandem with self-tracking experiments.

Such a narrative is oriented not towards a body of code, a body of numbers, or even objective certainty through machinic sensibility, but a lived experience of augmenting and recalibrating the conscious I. The ideal subject is here described as someone for whom "the data has moved inside [them]" (Nafus & Sherman 2014, p1788). (It is, in fact, the traditional medical relationship that is characterised as instrumental; we hope for the doctor's prescription to just 'fix' us then we can go back to not worrying about – or 'knowing' – our body again.) To be sure, this experience still involves using numbers and regular measurements to impose an order on reality. But the numbers are treated less as a window unto unmediated reality than an internally consistent set of relationships that can be manipulated.

In short, these debates and criticisms consistently point towards a common ground: a felt shift in the status of human experience admist advancements in machinic sensibility. And that shift, insofar as it alters the rules of the epistemic, truth-telling game, raises a normative and ethical problem: what kind of self-knowledge is knowledge produced through self-surveillance? What kinds of uncertainties are concealed in order to socially construct

tracking data as objective and accurate? To unpack these concerns, it is necessary to obtain a more historical perspective.

KNOW THYSELF

> Monday evening, I ate a cabbage and an omelet. Tuesday evening, I ate one half of the head of a kid and soup. Wednesday, fasted. Saturday, I went to the tavern: salad and omelet, and cheese, and I felt good. [64]

In January 1554, the Italian painter Jacopo Pontormo began to write. His topics: food intake, social calls, bowel movements, self-diagnosed psychological states. A few decades later, the physician and inventor Sanctorius of Padua would track his weight, his food (input) and excretions (output). Both would later be duly referenced as early precursors to 21st century self-tracking (Swan 2013; also see Urist 2015). Benjamin Franklin, with his thirteen virtues, also made frequent cameos in journalistic coverage of self-tracking (Kronsberg 2013). Self-trackers of the twenty-first century were not left wanting when it came to historical precedents, even if we limit ourselves to Western civilisations. Although contemporary discourse tended to make little more than cursory mentions[65], they provide an important point of comparison for understanding the epistemic and subjective (that is, for-the-

[64] The quotations are selected from Elizabeth Pilliod (2005)'s analysis of Pontormo's Diary.
[65] One exception is a lengthier discussion of weight scales, and their penetration into domestic spaces, around the turn of the 20th century (Crawford et al. 2015).

subject) stakes of self-tracking techniques. While a comprehensive history of self-tracking practices is well outside the scope of this work, this section focuses specifically on major practices and philosophies of self-knowledge in Antiquity, and then brings this comparative eye back to early twenty-first century debates about self-tracking and automation. Here we take the cue from Michel Foucault, who positioned these Antique techniques in terms of *parrhesia* and avowal – that is, techniques of truth-telling (Foucault 1986; 1997; 2001; 2011; 2014a; 2014b). Rather than take the vast difference in technological capacity as the primary point of comparison, I emphasise the different kinds of epistemic relations, different distributions of veridical authority, that can constitute a process of self-knowledge.

The Delphic maxim, 'know thyself' [γνῶθι σεαυτόν], is something of an unofficial catchphrase for the Quantified Self; Gary Wolf used it to title one of his own efforts to depict QS for the wider public, writing for his home publication *Wired* (Wolf 2009b). Originally, of course, the maxim was popularised through Plato's writings on Socrates. In this historical context, γνῶθι σεαυτόν described Socrates' methodology as much as the objective. If

to know myself was the ultimate objective, the second-person imperative[66] expressed the nature of the epistemic *process*. Briefly put, the subject would come to know oneself through the challenge of the speaking interlocutor, and in one's dialogic, experiential encounter with that challenge. Consider *Laches*, one of the Socratic Dialogues. Here, Socrates is described as an excellent interlocutor – that is, a human *medium* and indeed 'technology' for others' pursuit of self-knowledge. Instead of machines, he shall be the tool. But Socrates is qualified for such a function not due to his erudition, but a certain relationship he has cultivated between his actions and speech – that is, his conscious 'I' – and his *self:*

> When the life (*bios*) of the person speaking is in harmony with his discourse, when there is a symphony between someone's discourse and what he is, then I accept the discourse […] Laches does not say: Socrates is qualified to talk about courage because he is courageous. [Rather, he does so] because there is this symphony, this harmony between what Socrates says, his way of saying things, and the way in which he lives. (Foucault 2011, p148)[67]

This truthful relationship, this harmony, is encapsulated by the term *basanos* [βάσανος]. The term originally applied to a a silicon-based 'touchstone'

---

[66] γνῶθι is the command form of knowing, learning, becoming acquainted with; σεαυτόν is the reflexive pronoun, 'of yourself'.

[67] Laches says: "I have no acquaintance with the words of Socrates, but … have had experience of his deeds, and there I found him a person privileged to speak fair words and to indulge in every kind of frankness." (Plato 1920, p64 [188e])

which the Greeks used as a 'base' to test the purity of precious metals. In this context, it is Socrates who functions as a touchstone for others like Nicias and Laches. His questioning, and his own relationship to himself, stimulates, provokes, draws out, a kind of introspection and insight that they may not have arrived at themselves.[68] The crux here is the form of the *test*. If contemporary self-tracking tests users according to its pre-designed algorithms and classifications, the test here is intersubjective and dialogic. Socrates' subjects are not *told* what is right and wrong, or what the 'answer' to the question they face consists of. There is no informational transfer in that sense. Instead, there is a lived, communicative, asymptotic process by which the way one considers courage, the way one should approach such a problem, and the way one reflect upon oneself, is transformed.

The point here is not that modern self-trackers have a different experience of knowing, but that the *function and significance* of that experience itself is valued differently in comparison to older processes. Socrates makes this very point in *Phaedrus*, where he inveighs against the relatively new and destabilising technology of writing. He warns of the dangers of writing as

[68] Foucault (2011, p145) thus notes that *basanos* is derived to give *basanizesthai* [βασανίζεσθαι], the verb for a kind of being examined or tested. The latter form appears in Laches, most clearly in the Jowett translation: "To me, to be cross examined [βασανίζεσθαι] by Socrates is neither unusual nor unpleasant" (Plato 1920, p64 [188a]).

technology, arguing that such a radical increase in external mnemonic objects will take away from people's ability to remember 'of themselves'. But what is remembering 'of ourselves', anyway – and what, if anything, is lost if remembering becomes something done 'for us'? Once again, the problem comes down to the role of experience in epistemology. My recollection of a simple fact may be indistinguishable from a Googled result if we consider the end product as information. But there is all the difference in the *role* played by the subject in its own knowing.

> I cannot help feeling, Phaedrus, that writing is unfortunately like painting; for the creations of the painter have the attitude of life, and yet if you ask them a question they preserve a solemn silence. And the same may be said of speeches. You would imagine that they had intelligence, but if you want to know anything and put a question to one of them, the speaker always gives one unvarying answer. And when they have been once written down they are tumbled about anywhere among those who may or may not understand them, and know not to whom they should reply, to whom not: and, if they are maltreated or abused, they have no parent to protect them; and they cannot protect or defend themselves (Plato 1899, p581 [275d-e])

For Socrates, the chief sin of writing as a technology for instruction and knowledge is its ossifying quality: wisdom, unmoored from the process of becoming-wise, is abused through indiscriminate circulation. Socrates asks: do we not already know a better way to know and remember? "An intelligent word graven in the soul of the learner, which can defend itself, and knows

when to speak and when to be silent"? In this formulation, writing's production of stable, unchanging information is analogous to self-tracking's reliable, autonomous facts: the solid, data-driven assertion that you are depressed, or that chocolate makes you more productive, that does not change and transform with the weather or the caprice of my own perception. But it is precisely such stability that Socrates warns against. For him, knowledge is nothing without the transformative struggle that is the experience of knowing. The contrast we witness here is a derivation of what Plato called *anamnesis* and *hypomnesis*: between a lived convergence of history and experience on one hand, and an exteriorised memory of pure, disembodied information on the other.[69]

This is not to say that technological mediation pushes us from *anamnesis* towards *hypomnesis* in a linear fashion. Though Socrates was rather harsh on writing, a host of writing-based techniques for self-examination in late Antique and early Christian periods sought precisely to produce its own kind of dialogic, transformative experience. Foucault makes the point clear with Athanasius' *Viva Antonii* (typically anglicised as 'Life of Antony', c.360 AD),

[69] Also see Bernard Stiegler (n.d.) for a reading of Plato's binary in terms of modern technologies and externalisation.

an early Christian piece on the subject: "what others are to the ascetic in a community, the notebook is to the recluse". (Foucault 1997, p208)[70] In writing *as though* one was reporting to another, early self-writers sought to keep a check on their daily living. Just as other humans or machines examine and 'nudge' our conduct, writing was here designed to enable the subject to keep check on one's own soul. Precisely because writing gives 'one unvarying answer', it is a technology by which my own words can speak *back at me* as an other – that is, "establis[h] a relationship of oneself with oneself" (ibid., p211). Accordingly, self-writing in this period was typically a rigorous, regulated, disciplined practice. Seneca writes in *De Ira*:

> The spirit ought to be brought up for examination daily. It was the custom of Sextius when the day was over, and he had betaken himself to rest, to inquire of his spirit: 'What bad habit of yours have you cured to-day? what vice have you checked? in what respect are you better?' […] I daily plead my cause before myself: […] I pass the whole day in review before myself, and repeat all that I have said and done: I conceal nothing from myself, and omit nothing: for why should I be afraid of any of my shortcomings, when it is in my power to say, 'I pardon you this time: see that you never do that anymore'? (Seneca 2012, Book III, XXXVI)

[70] Foucault's commentary draws primarily on *Viva Antonii* §55, where Saint Antony [Antonius] advises others on how to maintain virtuous behaviour without the surveillance of others: "Let us each one note and write down our actions and the impulses of our soul as though we were going to relate them to each other… Wherefore let that which is written be to us in place of the eyes of our fellow hermit" (Athanasius 1987).

Such examinations were to occur regularly, at the close of each day. Foucault (1986, p61) notes that these sessions were held in an 'administrative' spirit, rather than guilt-wracked, emotionally overwhelmed penitence. The point was not to flog yourself in the eyes of God (or yourself), but to produce a reliable and accurate – it would be anachronistic to say 'objective' – form of self-knowledge. And so, with such self-writing, we find: the temporal and procedural regularity of the examinations; the model of the pseudo-rational, controlling I; the 'administrative' attitude as an affective regulator. These elements were designed to substitute the figure of the interlocutor with a relationship where I, in a specific sense, become other to myself. Where dialogic models provide an intersubjective other, through whom I come to know myself, exercises like Seneca's instantiate a nonsubjective other in the form of a disciplined, regulated relationship. Again, the emphasis is squarely on cultivating a subject that is then in a position to properly perceive and internalise their own truths; whether in Socratic dialogue, Seneca's examinations, or the alleged superiority of oral over written communication, there is no meaningful self-knowledge outside the subject's experiential relationship with his/her own self. Again, it is not the specific *content* of the experience that is conserved across these cases, but experience's centrality to the epistemic process. The experiencing I – as *basanos,* as 'administrator' – acts

as a clearing house for producing, curating, and analysing data about the self. It is this function that contemporary self-tracking attempts to bypass and undercut in its promise of automated objectivity.

***

And so we return to one of self-tracking's two distinct 'selling points': automation. Even as utopian visions surrounding 'smart' machines and persistent sensing construed the bypassing of human sensibility as an advantage, QSers and other practitioners of data-driven surveillance were beginning to caution against the dangers of defaulting to automation. All technological objects involve some degree of automation, of course. From Heidegger's hammer to voice-activated personal assistants in 2010's smartphones, each technological achievement is the result of human effort to set up an objective arrangement – machinic, algorithmic, material – that allows us to defer some part of the desired process, and all the information and skills and labour required therein, to the objects. The problem is that even as these autonomous sensing technologies promise to shine new light upon the unknown aspects of the self, the technological objects – data included – themselves become a black box.

> …what do we want to make more automatic? What do we not want to make automatic? What happens when things become automatic is, all the decisions that were in [that thing] sort of disappear [sic], and they become objects for the world that just feel like, they sort of landed in the world, and they do what they do. And it's hard to unravel it and unpack it, and make it do something different. And I think in our own lives, we have a lot of things like that, and we just say, I don't want to think about that, I'm just gonna do it. If it works for me, you know, and... and when do we say, you know what, I don't want to be on automatic pilot, I want to think about this? (Gary Wolf, 2015, personal communication)

Other ethnographic accounts point to similar discussions amongst QS members. For instance, Nafus and Sherman (2014, p1789) cite a 2012 QS conference discussion about the importance of manually entering data: "when it's all automatic, you aren't really aware of what it is saying". Such concerns recognised that automation often entailed a gradual evacuation of the experiencing I from the epistemic process. One response amongst tracking connoisseurs was to cultivate an ethic of DIY experimentation. Even as more and more automated devices entered the wider consumer market, many Quantified Selfers continued to cobble together their own tracking systems, or simply hack existing ones to their own particular purpose. These individualised solutions were sometimes as basic as manually recorded excel spreadsheets, or even sporadic entries in a paper journal about critical events and thresholds. This comparatively less rigorous form of recording was not

necessarily seen as a problem; it was accepted that self-tracking's well-documented goal of *personal* knowledge and *personally owned* knowledge often required a degree of practical know-how on the part of the tracking subject. Those who spoke of the importance of manual data input, or of a 'QS mindset' that can survive the cessation of actual tracking, thus understood that this lived struggle with different kinds of tables, variables and sensors is the modern correlate to the experience of knowing in Socratic dialogue or Seneca's self-examination. The tacit knowledge of the tracking subject thus became one way in which the vision of personal and agentic control sought to cohabit with the push for more powerful technologies.

Yet such experimentation was not expected to translate into the wider populace. By the mid-2010s, some QSers and QS observers were warning that mass-produced, mass-promoted versions of self-tracking tools would eclipse this experimental and experiential dimension. Thus Natasha Dow Schüll, an STS scholar that has studied both QS and self-tracking more widely, sounds a warning in *The New York Times*:

> 'There is this dumbing-down, which assumes people do not want the data, they just want the devices to help them," Ms. Schüll observes. 'It is not really about self-knowledge anymore. It's the nurselike

> application of technology.' In the move to the mass market, it seems, the quantified self has become the infantilised self (Singer 2015).

We began this chapter by noting that self-tracking technologies typically made two major claims to superior value: automation and intimacy. Yet these minoritarian views raised significant challenges against the theory of a virtuous synergy between the two. The utopian vision of self-tracking idealises an autonomous and machinic extraction of objective truth from the empirical 'me'. In stark contrast to Antique practices, this focus on what one's sleep *really* is like or how one *really feels* about one's friends increasingly positions the experiencing subject as a *consumer* of his/her own self-knowledge.

This 'consumption model' of self-knowledge sets up a telling parallel between corporate surveillance online and self-surveillance. In the 2011 QS Conference, Kevin Kelly's plenary talk acknowledged that "there is a thin line between the quantified self and 'intimate surveillance'".[71] If self-tracking promises deeper knowledge of ourselves through prosthetic machines that accompany us to meals, runs and sex, this very 'intimacy' is opening up new

[71] The quotation comes from Ethan Zuckerman (2011)'s liveblogged notes; Kevin Kelly confirms the accuracy of the notes in (Kelly 2011).

vulnerabilities for the subject's right to speak for his/her own self. In the case of corporate data-mining, such intimacy has already resulted in a 'Faustian bargain': the very means by which individuals are able to 'upgrade' their access to knowledge is the means by which their personal data is collected, monetised, and used to profile them (Zimmer 2008; also see Van Dijck 2013). In the Web 2.0 ecosystem, personal intimacy and economic intimacy are tightly intertwined, a conflation that dates back to mid-20th century computing discourse (Hu 2015). It is too early, and too sweeping, to declare that self-tracking is the latest trick up neoliberalism's sleeve, a way to turn us all into optimising and learning machines. As we have seen in this chapter, the meaning and uses of this technology remains very much contested. What is already visible, however, is a powerful directionality towards machinic sensibility as the alleged harbinger of objectivity – and, as its 'side' effect, an epistemic process that shunts intuition and experience into the periphery.

In Chapter 1, we characterised the epistemic relations in the Snowden Affair as 'recessive': a proliferation of objects which materially anchor a promise of data-driven knowledge, but in doing so, visibilise the uncertain and unknown elements undergirding those new epistemic techniques. While it does not roam quite so openly, uncertainty is just as central to self-surveillance's claims

of 'better knowing'. Here, uncertainty clings as the necessary inverse to the grandiose rhetoric of objective truth, of certainty achieved through machinic sensibility. Even as self-tracking imagines, and increasingly deploys, a system of automatic and intimate surveillance, the knowledge it produces - and the process through which it does so – is externalised away from the subject, rendering his/her own self-knowledge increasingly inaccessible. Meanwhile, the scattered complaints and anxieties against quantification, datafication, automation are syptomatic of another problem: the quest to eliminate uncertainty in the truth of the individual risks also eliminating a kind of freedom, a freedom for self-determination and transgression. Having thus identified the entanglement of knowledge and uncertainty in the social life of new surveillance technologies, the next two chapters ask: what kind of knowledge is nevertheless made to count, and is promised as possible? What kinds of techniques, beliefs, heuristics, are developed to ensure the legitimacy and possibility of knowledge? And although self-tracking discourse insists on bypassing the thinking I, ultimately, the subject and his/her responsivity is always at the end of every epistemic and communicative chain. In Chapter 4, we will come back to the demands that the ideals of machinic sensibility make of the human subject.

3. Knowledge Simulations.

'We knew already'. Or at least, that was the frequent refrain in the immediate aftermath of Edward Snowden's leaks on NSA surveillance. Did he tell us anything we didn't know? Asked journalists (Milner 2013). "They didn't feel much like revelations", said a director (Laskow 2013). It was as if this young man had risked his life to deliver shocking new revelations, only to find it was in fact rather predictable and dated. Snowden himself expressed the thought: in his encrypted communications, even as he invited journalists to Hong Kong for the now-famous exposé, he wrote of the fear that the public will simply 'shrug' and say, "we assumed this was happening and don't care." (Greenwald 2014a, p19) But what is meant by this curious phrase, *we knew already*?

'Knew' – yes, some of the information really was public knowledge. The *New York Times* had blown the whistle on warrantless eavesdropping as early as 2005; *USA Today* followed up with the story of MAINWAY, a domestic phone call records collection program, in 2006. John Poindexter, a key figure in the notorious Iran-Contra affair in the 80s, simply showed up to a DARPATech

conference in 2002 and publicly introduced state initiatives towards 'Total Information Awareness'. Even the entirely new aspects of state surveillance were, the discourse went, not very surprising: surely we expected things like PRISM as well, and Snowden just confirmed what was *virtually known*. But who is this 'we'? The discourse designates a depersonalised hivemind: the knowledge of NSA surveillance was stored in our collective archive, though the proof is in nonhuman documents rather than what individuals can 'remember'. Specific persons might well be surprised by the Snowden revelations, the idea goes, but the amorphous, collective 'we' did have the information available. Sometimes, the 'we' does become more specific. It designates the journalist the director, the activist: the we in the know who pens these commentaries, the we that is less gullible than the average Joe, the we of the 'we told you so'. A 'we' that is certainly very different from the 'public', even as such texts invite the public to agree that 'we knew already'. Satire, as it so often does, brings these ambiguities into the open: 'We already knew the NSA spies on us. We already know everything. Everything is boring', opines a spoof news article on the subject (*Clickhole*, 2015).

The vagaries of this one cliché exemplifies the various practical ways in which a sense of *sufficient* knowledge is secured in the surveillance context. The first

two chapters had described the proliferation of uncertainties amidst the promise of total archival and objective truth. Recessive objects give the uncertain and unknown a public presence – a presence invested with a promise of knowability, a necessity for calculation, collection, datafication. In this chapter and the next, we turn to recessivity's regulation of what kinds of knowing might be considered legitimate and useful, and to produce techniques or heuristics that human actors may use to establish a sufficient sense of knowability. In the context of state surveillance, the interplay of surveillance's secrecy and terrorism's unpredictability produces a host of deferred and simulated knowledge practices. Beneath the utopian banner of totalising archives and unprecedented predictivity, such techniques seek to fill the epistemic gap between the public and the secret surveillance system, between the fantasy of total prediction and the unpredictability of the twenty-first century terrorist. Here, the question is how recessivity's epistemic gap is sutured to enable a set of 'sufficient knowns': that 'we knew already' (even if many subjects, individually, did not) about state surveillance, or that the efficacy of surveillance can be 'reasonably' assumed (even if, in many cases, it cannot be proven).

In this chapter, we examine three knowledge techniques, three heuristics prevalent across both sides of the Snowden Affair: subjunctivity, interpassivity, and zero-degree risk. Subjunctivity describes an 'as if' form of reasoning, whereby knowledge and proof is deferred to a future or otherwise hypothetical state. Although a surveillance program may not yet have caught a terrorist, or brought about an Orwellian dystopia, subjunctive logic posits that the very absence of certainty *requires* the public to act on uncertain evidence. One particularly consequential rendition of subjunctive reasoning is in what I call *fabrications*: a post-September 11 tendency in surveillance and counter-terrorism to support and encourage suspects until the suspicion is coaxed into tangible proof of wrongdoing. The chapter then describes interpassivity: the idea that one does not know, or has not done anything wrong, but 'someone else' – or even some*thing* else – has in my stead. If subjunctivity leverages potentiality to actualise uncertain claims to knowledge, interpassivity looks to the human and nonhuman Other – from the vast depths of the NSA database to secret courts that supposedly know in the public's stead. Finally, zero-degree risk returns to the fixation with numbers and statistics that we had observed in Chapter 1. In the Snowden Affair, the difficulty of rendering surveillance and terrorism calculable has in fact coincided with a proliferation of numbers and probabilities; in other

words, the *performative* quality of risk discourse and statistical reasoning contributes to the normalisation of 'acceptable levels' of uncertainty and speculation.

These techniques describe, respectively, three sources of epistemic authority that 'fill in' for the proliferation of uncertainty in the surveillance context: potentiality, the Other, and numerical empiricism. To be sure, modern epistemes have always entertained a host of heuristics to stabilise claims to knowledge. The simulations described here are well recognisable in other contexts, from the authority granted experts in modern societies (e.g. Giddens 1990; Debord 1990, VII) to similarly uncertain problems like climate change. The chapter's focus is not on introducing entirely novel phenomena, but understanding their function vis-à-vis the constantly shifting distribution of epistemic authority and the boundaries of knowability. From the FBI's turn towards actively manufacturing terrorist suspects (a practice which they had not previously engaged with such frequency and enthusiasm) to surveillance discourse's shedding the pretense of calculable risk and probabilistic reasoning, these techniques detail a visible turn towards increased dependency on simulated knowledge by state surveillance actors. And as with the recessive objects in Chapter 1, this increasingly explicit entanglement

between 'sufficient' knowledge and the unknown is not limited to a particular political position, but replicated across both the advocates and critics of surveillance. Subjunctivity, interpassivity and zero-degree risk are thus crucial operators in surveillance's bid to both project massive uncertainties and the technological promise of better knowledge. They are best understood not as irrational and deceptive manipulations of knowledge processes, but part of the constant redrawing of normative rules that govern what relations of deferral, simulation, speculation, come to 'count' as knowledge.

SUBJUNCTIVITY

> Your rights matter because you never know when you're going to need them. People should be able to pick up the phone and call their family, should be able to send a text message to their loved one, buy a book online, without worrying how this could look to a government possibly years in the future.
>
> -Edward Snowden (Rowan 2014)

> I buy fire insurance ever since I retired, the wife and I bought a house out here and we buy fire insurance every year. Never had a fire. But I am not gonna quit buying my fire insurance, same kind of thing.
>
> -James Clapper, US Director of National Intelligence (Lake 2014)

The distilled formula: you never know, so you have to do something. Both the whistleblower and the public face of NSA surveillance speak the language of *loomings*: threats that are nothing *yet*, but are already very much *real* in their existence as potential (Massumi 2005, p35). They invoke the Orwellian future

where you might be punished for the ordinary actions taken today; the apocalyptic scenario when terrorism happens to *you* with a ruthless individualisation. That which by definition cannot ever be made certain is invoked as presumptively real in order to legitimise action, whether for or against state surveillance.

This is the *as-if*, the subjunctive. Grammatically, the subjunctive mood invokes a statement that it explicitly acknowledges as hypothetical or unproven: 'if I were…' It joins the explicit acknowledgement of a given thing to be unproven or presently non-actualised, *and* nevertheless gives it an operational reality for decisions, sentiments and predictions. Does James Clapper believe there is going to be a fire, or not? The subjunctive construction dismisses such binarism, and invites participants to accept that even if the fire may never happen, it is sufficiently disastrous that we must consider it a real basis for judgment and action. Uncertainty here is not counted as a penalty upon the quality of the proof, a negative lack of information, but an aspect of social reality in and of itself which demands a (rather certain) response.

The as-if is a common fixture in our language use across multiple media. In news photography, for example, the frozen image of a conflict, a wound, a death, serve to – provoke an emotional and speculative relationship to the information at hand, to consider: what might have happened after the photograph was taken? What could be happening in that conflict zone right now? (Zelizer 2010, p12-15) Entire genres of communication engage in the business of concretising the non-actual, rendering them affectively, discursively, available for operationalisation. In science fiction studies, Samuel R. Delany defines subjunctivity more broadly as "the tension on the thread of meaning that runs between" words; a "blanket indicative tension (or mood) [that] informs the whole series", infusing the situation with a hypothetical presence. In these terms, the as-if of the Snowden Affair constitutes a kind of science fiction – a fiction that concerns itself with 'events that could have happened', whereas fantasy, for instance, concerns things that 'could not have happened' in our universe (Delany 1971 p10-11). And despite science fiction's traditionally low position in the cultural hierarchy, there are numerous historical linkages between its speculative theorising of our future and the real social history of computing and the Internet. Spacewar, MIT's 1962 video game that emblematised the move towards personal, real-time, 'free' cultures of computing (Hu 2015, Chapter 1), was at the time strictly

envisioned as a nonorthodox attempt at applied science fiction (Milburne 2015). The hacker-troll-activist collective Anonymous hit upon the 'Guy Fawkes' mask as its symbol through the Hollywood blockbuster V for Vendetta (Coleman 2014, p64), as well as the 'Laughing Man' from the Japanese sci-fi manga Ghost in the Shell (which, in turn, derived the figure from J.D. Salinger's *The Laughing Man*). We shall see throughout the chapter how narrativisations of totalitarian surveillance, of ubiquitous terror threats, of suspects that just *had to* be stopped before they could conclusively prove their own guilt, all entail such leveraging of 'fiction' to render a mysterious and dangerous reality meaningful.

In other words, subjunctivity often produces grey areas for bestowing speculative and hypothetical reasoning a disavowed form of veridical authority. Timothy Melley (2012) points out that the many secret institutions, practices, policies that make up the dark side of the US government – surveillance included – are often leaked into the public sphere through fictional literature and the use of speculation in official public discourse. He argues that the result is a public sphere of 'structural irrationality': as truth becomes regularly accessed through fictional detours (that are again explicitly known to be fictional-but-serious), there is contamination of the public use of

reason, or rather, a public faith in rational proof. But I do not want to speak the language of irrationality, if only to avoid a different kind of ideal fiction: that of the 'normal', properly rational knowledge purged of speculation. The point is that subjunctivity brokers the manifold connections between speculations about the explicitly uncertain and nonactual on one hand, and the operationalisation of knowledge – that is, turning knowns and certainties into judgment and action – on the other.

These characteristics mark deployments of subjunctivity as highly ritualistic. Rituals have been called 'time out of time' (Rappaport 1999, p216-222), or liminal (Turner 1982) zones. They are moments which say, wait: let us step out of our rules and rhythms of life for a moment, so that they may be renewed and reaffirmed, or undergo localised changes (such as the change in status of an individual member in a rite of passage). In the Snowden Affair, we find subjunctive constructions that allow the audience to 'play out' totalitarian futures and next terrorist attacks – constructs where the boundary between such speculation and reality is even more porous. The simple refrain that 'you never know' thus invites the public to suture scenarios and simulations back into their assessment of 'reality'. In context of the proliferation of unknowns that characterise early twenty-first century

electronic surveillance, subjunctivity offers the public one way to reconcile its enduring uncertainty about what it is supposed to have 'known already'.

***

As with recessive objects, the basic uncertainty underlying the Snowden Affair as an epistemological problem is that the individual can never be sure if he/she has been surveilled. This is the first as-if. The recessive juxtaposition of an apparently enormous and pervasive surveillance system, and the fact that the surveilled subject will rarely know if they have ever been 'watched' by a human agent, means that the public is essentially asked to generate outrage over something they cannot find any individualised trace of. Snowden and other opponents of NSA surveillance consistently attacked this recessivity – ironically, by projecting and combating another kind of as-if. Anti-NSA discourse consistently interpellated an imagined public which presumably thinks it is safe as long as it has not done anything 'wrong'. A New York Times op-doc, "Why Care About the N.S.A.?" opened with a stern warning from David Sirota, a well-known political commentator:

Narrator: I want to get your response to a few things people typically say who aren't concerned about recent surveillance revelations.

David Sirota: Nobody is looking at my stuff anyway, so I don't care? My argument for that is if you don't speak up for everybody's rights, you better be ready for your own rights to be trampled when you least expect it. First and foremost, there are so many laws on the books, there are so many stat-utes out there, that you actually probably are doing something wrong… So when you start saying I'm not doing anything wrong… you better be really sure of that. (Knappenberger 2013)

Figure 9. Legalese in flight.

Sirota's lines were accompanied by a dizzying array of legalese in flight (Fig.9). By shifting the subject's gaze onto the bureaucratic and technological depths which almost entirely lie beyond everyday experience, the subject is divested of the ability to confirm or deny his/her own safety. This is distinct from the simple claim that the public is not safe. Rather, it is argued that the

public does not have the ability or resources to *tell* in the first place. The projected 'common sensical' subject is appealed to through an indeterminate what if. The reality of surveillance is emphasised not by recovering concrete surveillance practices from their recession, but by expanding their virtual dimension into an enormous, totalitarian as-if.

This same technique is applied to the threat of terrorism. James Clapper quipped that PRISM is no different from fire insurance. But insurance developed its appeal by quantifying fearful indeterminacy into percentages and premiums. The strategic use of disaster statistics and risk percentages could *claim* to provide a stable and objectively factual knowledge of danger and vulnerability. As we shall see later in the chapter, such calculations are difficult to produce with respect to terrorism. In the face of a radically unpredictable threat, state surveillance has practiced, and justified itself on the basis of, a subjunctive reasoning: everybody[72] needs to be watched, treated as if they are suspect. One key metaphor for NSA surveillance programs is the *dragnet* – a term traditionally used to describe police activities

[72] As we noted in Chapter 1, this 'everybody' rarely means literally everybody. There is a general tendency to over-imagine the threat of the black, Muslim, male and mentally deviant – a tendency which is reflected in some state / local government operations. We might point to the NYPD's multi-year surveillance of Muslim neighbourhoods and Muslim-owned shops, seemingly purely for reasons of demographic, that ultimately yielded no solid leads and two lawsuits (See *Associated Press* 2012; Calamur 2016).

like location-wide stop and frisks. The dragnet indiscriminately collects data on the innocent as well as the suspicious, highly relevant data as well as irrelevant ones. After all, the innocent can always turn out to be the criminal, and the most irrelevant piece of data may help triangulate his/her identity. Within this rationality, surveillance is not, strictly speaking, proven to be necessary by *past* terror attacks or *present* identification of concrete dangers. Proof is always deferred: we must act as if the efficacy of this program has been proven by a danger which, if we are right, we will prevent from ever actualising. It is no surprise that many commentators have taken to *Minority Report* – more often the Steven Spielberg film adaptation than the original Philip K. Dick story – as a glossary for parsing the juridical and civil rights consequences of the NSA and its UK counterpart, the GCHQ (Burris 2016, Anthony 2015).

Subjunctivity is one name for how public figures *present* the world of surveillance. Importantly, this presentation is also a part of public subjects' epistemic relationship to that complicated and distant world. The public is enjoined to engage in subjunctive readings of media discourse on surveillance in order to navigate this tangle of complex and often contradictory claims. Consider the efforts to assess the legality of surveillance from the public end.

Snowden's revelations were, at least, generally accepted in the media as solid, reliable information about the technical process of NSA surveillance. However, the precise legality of each given practice, and indeed, the question of *who* actually knows about and guarantees each practice, was often explicitly designated as uncertain. As one headline put it: 'You'll Never Know if the NSA Is Breaking the Law' (Bump, 2013). On one level, it is suggested that there are so many different programs, legal decisions, secret courts and procedures involved, the public will 'always' be left uncertain as to its legality. On another level, we cannot presume that the reading public is a homogeneous mind with full access to every piece of information made available to them. The 'we' of 'we knew already' simply does not exist in such a simple form. Most subjects are likely to experience a partial picture, based on their limited reading and recall, of conflicting arguments and claims made in public. One may not keep up with every Snowden leak, tell apart XKEYSCORE from PRISM, or even understand exactly what counts as metadata and what doesn't. But it is more than possible to take away a general picture: the idea that the legality of surveillance is uncertain, and that any opinion or action we take will have to happen in abeyance of that knowledge.

All of this resonates with the paranoid structure of recessive relations. Chapter 1 showed how even as Snowden provides new information to the general public, his leaks also provoke further speculation – and for some, downright conspiracy. Media, in its constant exposés, cultivate in the public a "persistent feeling that 'there is always something" (Horn 2012, p118). In this context, subjunctivity is not just something we defer to when we feel that we are in the dark; it is also a way of making use of the information that we consider to be 'fully known' to further speculate upon what remains unknown. The US state surveillance system is vast – and it is far from being a singular system at all, comprised as it is of tens of thousands of employees and private contractors. Since such a complex and secret apparatus cannot ever be fully accounted for in public, subjunctivity becomes a way to constantly approximate the dark side of the known. In this way, one journalist applied the lessons of the Snowden leaks to speculate on the presidential contest between Barack Obama and Mitt Romney in 2012:

> Did the Obama Administration ever spy on Mitt Romney during the recent presidential contest? Alex Tabarrok, who raised the question at the popular economics blog Marginal Revolution, acknowledges that it is provocative. Until recently, he would've regarded it as a 'loony' question, he writes, and he doesn't think that President Obama ordered the NSA to spy on Romney for political gain.

> Let's be clear: I don't think so either. […] But I agree with Tabarrok that today, 'the only loonies are those who think the question unreasonable.' Most Americans have a strong intuition that spying and electoral manipulation of that kind could never happen here. I share that intuition, but I know it's nonsense: the Nixon Administration did spy on its opponents for political gain (Friedersdorf 2013).

The rhetoric goes: no, Barack Obama probably did not spy on Mitt Romney; but yes, the threat is real, and the threat is to be communicated in the form of this spying that did not happen. Paranoid epistemology is thus *recommended* as a realistic and timely response to the available facts. In 2015, *The Atlantic* ran an exemplary piece named "If you're not paranoid, you're crazy":

> Not long ago, my wife left town on business and I texted her to say good night. 'Sleep tight and don't let the bedbugs bite,' I wrote. I was unsettled the next morning when I found, atop my list of e-mails, a note from an exterminator offering to purge my house of bedbugs. If someone had told me even a few years ago that such a thing wasn't pure coincidence, I would have had my doubts about that someone. Now, however, I reserve my doubts for the people who still trust. There are so many ghosts in our machines – their locations so hidden, their methods so ingenious, their motives so inscrutable – that not to feel haunted is not to be awake. That's why paranoia, even in its extreme forms, no longer seems to me so much a disorder as a mode of cognition with an impressive track record of prescience (Kirn 2015).

The anthropologist Mary Douglas once asked: why do experts insist on educating the public about issues like climate change? Don't they realise that the more information becomes available, the more possible interpretations

arise, and the more intractable a sensitive topic becomes? (2001, p. 146) The proliferation of subjunctive reasoning is one way in which information and uncertainty enters into a mutually generative relationship.

***

Subjunctive reasoning was popular not only in the media conversation and the challenges faced by intelligence agencies, but in the everyday techniques offered to citizens as a way to protect themselves from surveillance. Since the initial leaks, Edward Snowden embraced his new name recognition with the wider public by dispensing advice on how to stay safe in this newly dangerous (Or rather, newly realised to have been dangerous) digital world:

Micah Lee:	What are some operational security practices you think everyone should adopt? Just useful stuff for average people.
Edward Snowden:	[…] The first step that anyone could take is to encrypt their phone calls and their text messages. You can do that through the smartphone app Signal, by Open Whisper Systems. It's free, and you can just download it immediately. And anybody you're talking to now, their communications, if it's intercepted, can't be read by adversaries […] You should encrypt your hard disk […] Use a password manager […] The other thing there is two-factor authentication (Lee 2015).

Operational security, or OPSEC, in fact originates from the US military. The US Department of Defense defines it as "the process by which we protect unclassified information that can be used against us" (*US Department of Defense Education Activity* n.d.). In effect, Snowden is adding to our already lengthy list of practices that constitute our 'digital hygiene': the things the individual user must do to "kee[p] her data from mixing with others, for avoiding infection with computer viruses, and so forth." (Hu 2015, p57) But these practices themselves enact a recessive, simulational relationship. Consider AVG PrivacyFix (Fig.10), one of many simpler tools which promise to protect against state and/or corporate surveillance. It is all too easy: a few clicks, yellow and white symbols flashing into a reassuring green, and one is allegedly safer. Certainly, there is no doubt that, say, opting out of Google's peer-recommended ad system (where your reviews and comments are used to sell the product to your friends) restricts the commercial exploitation of your personal data, of your trace-body. But when privacy tools proudly inform you that 42,787 trackers have been blocked so far, or that your worth to Twitter has declined from $30 to $25, such feedback emphasises the fact that the user cannot directly perceive the myriad of threats they are exposed to. This is also the case with examples like alternative webmail or instant

messaging services (Greenberg 2014). 'Digital hygiene' begins to replicate our modern relationship to health and hygiene: just as 'health' is merely a temporary and relative freedom from pathologies, into which we may slip back at any moment and therefore require our unending vigilance, there can be no escape from the threat of surveillance (Hacking 1990, p160). Edward Snowden himself acknowledges the impossibility of becoming 'clean':

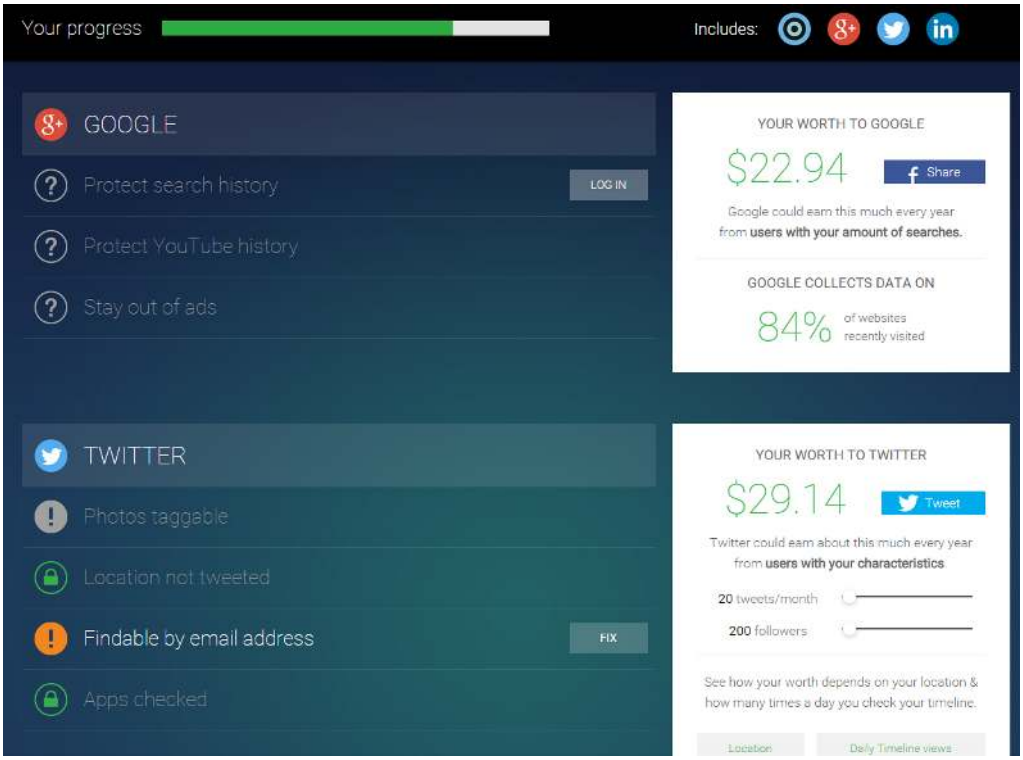


Figure 10. AVG PrivacyFix.

> You will still be vulnerable to targeted surveillance. If there is a warrant against you if the NSA is after you they are still going to get you. But mass surveillance that is untargeted and collect-it-all approach you will be much safer [with these basic steps] (*Inside.com* 2014).

In other words, the subject's feeling safe enough is predicated on his/her ability to live on as if whatever tools chosen (including none) has provided sufficient protection against this unknown and silent risk. While we can generally never know if someone has hacked into our email and read its contents, subjects are invited to prepare as if the worst will happen – and then, proceed with our life as if we know we are now safe. It is significant that Snowden and other activists view the difficulty and complexity of most privacy tools as the primary barrier against their wider uptake, and look forward to a future where they become unobtrusive, backgrounded. There is a clear parallel between self-surveillance devices and privacy tools for digital hygiene: in both cases, the pressure to achieve widespread 'buy-in' ends up promoting a black-boxed understanding of the battle over data. Good hygienic citizens, just like good self-caring, self-managing citizens, are educated towards not a radical break with data-driven epistemology or genuine expertise, but an allegedly 'healthier' mode of engagement and dependency.

> Edward Snowden: We should armor ourselves using systems we can rely on every day. This doesn't need to be an extraordinary lifestyle change […] It should be invisible, it should be atmospheric, it should be

> something that happens painlessly, effortlessly. This is why I like apps like Signal, because they're low friction. It doesn't require you to re-order your life […] You can use it right now to talk to your friends (Lee, 2015).

This is not to say that more radical forms of resistance are ideal. Consider the practices of camouflage, protest and reverse-watching that have sometimes passed under the name of *sousveillance*: *sous* (below) + *veiller* (to look).[73] Artist Leo Selvaggio (n.d.) has produced a variety of mask kits – 3D printed photorealistic, paper cutouts, or in the form of software that maps the mask onto the user's face in video feeds – modelled after his own face as a way to resist CCTVs and facial recognition software (Fig.11). Such solutions join a larger group of non-practical demonstrations: the anonymous Surveillance Camera Man (n.d.) roams the streets, public spaces and private buildings of Seattle with a camcoder, raising the question of why many citizens respond so viscerally to his camera but passively accept top-down CCTVs.[74] Yet these practices, often staged by artists, clearly are not intended to replace digital

[73] Sousveillance need not be defined as political or resistant, and some have attempted to subdivide the practice through terms like 'inverse surveillance'. Here, we focus on strategies of watching back / surveillance-avoidance clearly designed to resist the proliferation of state and corporate surveillance.

[74] Such projects stylise surveillance resistance in a way that has been criticised as merely spectacular and fashionable 'aestheticisation of resistance' (Monahan 2015). While I do not entirely disagree, here I am concerned with highlighting their role in the broader imaginary of ubiquitous, hyperobjective surveillance.

hygiene and other ordinary habits. Even as such performances seek to 'raise awareness' about surveillance and 'provoke debate', they work to further visibilise surveillance as a kind of ubiquitous miasma.

Figure 11. Leo Selvaggio's face mask.

In Chapter 1, I had referred to 'public secrets': something which is widely 'known' but not articulated, such that one must actively 'not-know' (Taussig 1998). Public secrets essentially smuggle secrets into the public realm; by 'knowing what not to know', savvy actors can participate in the benefits of knowledge without giving the game away. Subjunctivity follows a similar

mechanism. It deploys what is formally hypothetical and unproven in the form of a disavowed knowledge. The as-if leverages the receded, virtual enormity of 'surveillance' to furnish an expanded field of what counts as knowledge.

FABRICATION

Subjunctive relations were not confined to media rhetoric, or even to the public's positioning vis-à-vis knowledge and secret. Subjunctivity's popularity in the public presentation of surveillance reflected a parallel turn towards potentiality and 'sufficient' proof in the American government's effort to mobilise surveillance for counter-terrorism purposes.

One key aspect of subjunctivity in counter-terrorism has already been subject to extensive research and commentary: the growing linkage of simulationionist and otherwise 'hypothetical' analysis for the purposes of anticipatory and pre-emptive interventions. From simulations of terrorist networks based on computational models (e.g. Moon & Carley 2007) to elaborately designed, physically enacted scenarios training civilians to respond to terror attacks (e.g. Adey & Anderson 2012), the US and numerous other states have expanded old techniques and developed new ones to

actualise and 'play with' the possibility of every kind of terrorist attack. These strategies sometimes directly enrolled the public, enjoining them to internalise and practice a form of 'lateral surveillance' (Andrejevic 2005) that some have described as banalisation of insecurity (Monahan 2010; Bauman & Lyon 2013). At other times, the state's simulations of dangers might intersect with the media and public imagination of dangers and of state simulations themselves, further normalising a subjunctive ground for debate and opinion. In 2015, a map used in the US military's 'Jade Helm' training exercises – which were already controversial – was leaked to the public, provoking commentary, speculation and conspiratorial interpretation. The map, detailing one of Jade Helm's mock scenarios, showed Texas as a 'hostile state', which friendly (labelled 'permissive') states like California and Colorado might help subdue (Davidson 2015). At the same time, a different rumour made the rounds – that concrete ISIS terrorist bases had been discovered in Texas. Senator Ted Cruz, "fresh from his Jade Helm inquiry", and in a few short months about to run for President on promises of being tough on Islamic terrorists, accused the incumbent government of failing to connect the dots. A mock military scenario and an unconfirmed rumour had mutually reinforced each other's status as half-truth, or rather, operationalisable fiction. One poll of registered Republican voters immediately following the leaks pegged 32% as "think[ing]

that the Government is trying to take over Texas" (*Public Policy Polling* 2015). The linkage between virtues of 'preparedness' and predictivity, and the practice of simulationist and otherwise hypothetical epistemologies, has emerged as a key facet of counter-terrorist strategies in early twenty-first century America (also see Adey 2009; Aradau & van Munster 2012; Anderson 2012; Massumi 2007, 2010).

This section focuses on one specific practice that intersects electronic surveillance and counter-terrorist efforts – one which exemplifies the subjunctive epistemology at the heart of practical operations. What I call *fabrication* is the deliberate, planned, and increasingly systematic practice of producing what sufficiently 'counts' as evidence in counter-terrorism operations. Here, surveillance combines with traditional human intelligence work to cajole, instruct, encourage, coax a suspected danger into something that can legally count as 'real enough' and thereby legitimise action. Such strategies have come to occupy a central role in the FBI's counter-terrorist operations since September 2001 – a shift which was accompanied by a belief that the uncertainties surrounding Lone Wolves-to-be had to be pre-emptively dispelled, and by a contemporaneous establishment of online

communications infrastructures[75] and large scale databases for informants (Aaronson 2013). While sting operations have been part and parcel of FBI operations for decades, fabrication blurs the distinctions separating sting ops from downright entrapment.[76] Assisted by telecommunications surveillance, and motivated by political pressure to prevent 'all' threats, strategies of fabrication exemplify the ways in which subjunctive reasoning is mobilised to legitimate specific practices for producing truth and certainty. The word 'fabrication' today applies a pejorative judgment to the original meaning – *fabricatus*, to construct, to build, to make. But it is not my intention to imply that all of this is a farce. In the context of New Terrorism, where one must grapple with inexhaustible unknowns and nevertheless force through a sufficient basis for knowledge and action, fabrication emerges as an eminently *sensible* and risk-conscious practice appropriate to a paranoid epistemology.

---

[75] The classic distinction between sting operations / *agent provocateurs* and entrapment is that in the latter, the subject is judged to have been predisposed to commit the crime regardless of government encouragement or facilitation – a distinction which in the United States is typically tested through both 'subjective' (was the subject predisposed?) and 'objective' (would the government's actions have pushed a 'normal' citizen to crime?) standards. I do not present fabrication as a third category in this general typology of law enforcement strategies. Rather, it constitutes a concrete example of subjunctive knowledge production at work in the state surveillance context, in the form of a localised derivation of existing production strategies in counter-terrorism and law enforcement institutions.

[76] As Aaronson (2013) recounts, the FBI had been so averse to computerisation on the operations side that before September 11, most agents could not search the Internet from their office computers, and informants were managed locally through personal relationships with agents.

***

In 2011, an FBI sting operation began to form around Sami Osmakac. A Kosovo-born American and Muslim, his trusted Muslim friend had introduced him to a man named Dabus, an FBI informant who in turn connected Osmakac to an undercover agent named 'Amir Jones'. To that point, Osmakac's record of suspicious activity included a tendency to verbally criticise democracy, argue for his religion in combative and fundamentalist terms – and one streetside fisticuffs with a Christian street preacher that had recently gotten him arrested. In other words, little in the way of convictable behaviour. After meeting Dabus and Jones, however, Osmakac was supplied with money, with which he could purchase (fake, prepared) weapons and explosives; he was trained in their use; and he was even given money for a taxi so he could show up to his own attack spot, where he was finally arrested by the FBI. During the process, the FBI agents spoke of Osmakac as a 'retarded fool' who needed the FBI's support to turn his 'pipe-dream scenario' into any semblance of a real threat – a result which they referred to as a 'Hollywood ending' (Aaronson 2015). The FBI provided material and psychological encouragement that allowed Osmakac to become 'dangerous enough' to be legally and operationally eligible for arrest. Of course, this also

means that it becomes impossible to ever confirm whether Osmakac would have acted without such encouragement; the price of a pre-emptive certainty is the absolute unconfirmability of justice. A similar strategy has been employed with numerous other American suspects.[77] One report estimates that around 30% of counter-terrorism convictions between 2002 and 2011 were fabricated through stings (*Human Rights Watch* 2014). In the case of José Padilla, a.k.a. Abdullah al-Muhajir, this subjunctive reasoning was sufficient to approve three years of detention without formal charges – and, possibly, torture (a claim made by Padilla and his lawyers and denied by the government). Paul Wolfowitz, the US Deputy Secretary of Defense at the time, made it clear that the state stands behind this new standard in preemptive action:

> There was not [that is, Padilla did not yet have] an actual plan. We stopped this man in the initial planning stages, but it does underscore the continuing importance of focusing particularly on those people who may be pursuing chemical, or biological or radiological or nuclear

[77] Osmakac thus joins other (predominantly, but not always, Muslim and/or of Arab descent) Americans whose antisocial, delusional or otherwise mentally non-normative conditions were relentlessly manufactured into apparent proof of violent intentions *and* the capacity to carry them through. Matthew Llaneza, for instance, was an American of Filipino, Anglo-Irish and Hispanic descent who was later described by an FBI informant as having 'the mind of a little child'. Having converted to Islam and grown a beard, his drunk ravings of *Allah Akbar* at a house party, combined with wild boasts about knowing how to build guns (despite being unable to rake leaves in the back yard as instructed), were treated very seriously in assembling charges against him. Eventually, he too was contacted by an undercover agent, encouraged to plot in words a bombing attack, and duly arrested (Bergen 2016).

> weapons. This is one such individual (Kozaryn 2002; also see Adey 2009).

Subjunctive reasoning has been central to the justification of fabrication strategies both internally and externally. The two dimensions come together in the case of Basaaly Saeed Moalin, a Somali American arrested in 2013. Moalin was a crucial case for the ability to publicly 'know' the benefits of surveillance. Although one or two other cases, like Najibullah Zazi's, had been cited as having prevented through dragnet surveillance, Moalin was – at the time of writing – the single known case, the single point of certainty, that could show the benefits of spying to ordinary Americans (Schwartz 2015).[78] Yet the construction of this claim to certainty was also predicated on strategies of fabrication. Arrested on charges of conspiracy and material support for terrorism – specifically, posting $8,500 to a Somali contact associated with the jihadist group al-Shabaab – the prosecution argued that Moalin's frequent phone calls and money transfers supported terrorism. Once again, Moalin had to be apprehended *before* he could produce any further certainty or concrete knowledge; it was argued that to wait for 'proper' proof would be unacceptably negligent of real dangers posed by the suspect.

---

[78] Moalin's case, at the time of writing, remains the only specific case where the American government has publicly cited a 'critical' reliance on NSA metadata surveillance. Of course, the qualifier is 'publicly'; the public has consistently been reminded, often by the state itself, that there must be additional proof that must remain secret.

In court, the defence directly contested this interpretation of available evidence – and in doing so, publicy exposed the fabrications as a set of uncertain and primordial indices *oriented* towards certainty. Picking apart Moalin's phone calls collected by telecommunications surveillance, the defence argued that his comments about 'jihad' referred to a local jihad in his native Somalia against the Ethiopians; that his money transfers to his homeland had gone to projects for schools and orphanages; and, indeed, that no record showed any definitive statement in support of terrorist attack (Nakashima 2013). The defense went as far to submit to the court alternative transcriptions to Moalin's Somali calls, and even enlisted cultural interpretations. Moalin's cousins argued that his talk was a well recognised form of *fadhi ku dirir* (literally 'sitting and fighting'), a bullish and aggressive but ultimately noncontroversial form of argumentation common amongst Somali men (Schwartz 2015). Since Moalin was apprehended before he could supply further certainty in the form of a violent attack or concrete statements referring to one, surveillance and arrest had to be justified through subjunctive and paranoid readings of relatively cryptic comments like the following:

BASAALY [Moalin]:	We are not less worthy than the guys fighting.
ISSA:	Yes, that's it. It's said that it takes an equal effort to make a knife; whether one makes the handle part, hammers the iron, or bakes it in the fire (from Schwartz 2015).

The palpable gap between Moalin's words and the eventual charges (of conspiracy and material support for terrorism) echoes the recessive relationships in the Snowden Affair. Fabrication thus fulfils the crucial role of constructing a rationality for subjunctive judgment and action. While some degree of fabrication is by definition a necessary part of any preemptive measure, this period saw a visible embrace of more speculative forms of knowledge that could license more actively interventionist efforts – largely because it was thought that the threats of New Terrorism did not permit the luxury of greater proof and certainty. If these suspects were being directed and shaped on the basis of potential rather than actual danger, operatives and politicians argued, so be it: such pre-emption is the only way to ever 'know enough' in time to stop the next attack. This attitude was founded in the recriminatory, zero-tolerance climate established by America's heightened sensitivity to terrorist threat in the wake of September 11.[79] Here we may turn

[79] We return to this doctrine, and its connection to the new conceptualisation of risks, later in the chapter. The idea that America "can't afford to wait", riding the crest of public concern over September 11, spread in this period to many areas of intelligence and military activity, including R&D funding for preventative measures in biological warfare (Cooper 2006).

to a third case: Ehsanul 'Shifa' Sadequee. In 2005, Sadequee, 19 years old, was arrested and sentenced to 17 years in prison for suspicious activity that largely comprised of translating jihad-related texts, talking big online, and producing a ludicrously amateur 'casing video' in Washington D.C. In Sadequee's case, there was no active fabrication, at least none that has been disclosed publicly; but it was another instance in which highly primordial activities and discussions, which might at most be said to 'encourage' terrorism, was mobilised to eliminate the target from social existence. In a rare moment, Sadequee's family journeyed to meet Philip Mudd – the man who had, as deputy director of the National Counter-Terrorism Centre at the time, had a direct hand in the case. Mudd, while courteous and sympathetic to Sadequee's family, insisted on the necessity of such an action:

> People like me are in a difficult position. We cannot afford to let dozens of innocent people die because a youth makes a mistake […] If we switched roles, what would you do? What would you do? Would you let him go? (Barker 2016)

The 'zero-tolerance' policy renders epistemic uncertainty intolerable. It is far less acceptable to respect the rights of suspects, because one cannot write off any attack as an 'acceptable' or unavoidable loss. And yet, in so many cases, especially that of lone wolves and 'home-grown' terrorists, the possibility of

crime remains uncertain until it is too late to intervene. Fabrication fills this gap, ensuring that uncertainties are coaxed into the realm of sufficiently known. Thus zero risk, worst case scenario, and the changing status and nature of 'proof' are all arranged to follow rationally from each other.

These trends within intelligence agencies and surveillance-driven counter-terrorism practices were complemented by a wider political and military of fabrication. Indeed, the problem of fabricating sufficient knowledge out of Moalin's communications is formally analogous to the most infamous case of speculative proof in the period: the alleged presence of weapons of mass destruction [WMD] in Iraq, which functioned as a crucial *casus belli* domestically and internationally for US invasion. In February 2003, Secretary of State Colin Powell famously presented the US administration's case for war to the UN Security Council. Amongst the 'facts and conclusions based on solid intelligence' (Powell 2003) he offered were foreign communications data intercepted by the NSA. In the first excerpt, an Iraqi colonel vaguely referred to "this modified vehicle … what do we say if one of them sees it?" In the second and third, there were equally broad references to "forbidden ammo" – and then, in a rare moment of relative specificity, an order to "remove the expression 'nerve agents' from wireless instructions." (Bamford 2008, p144)

From arresting Muslim American teens to justifying regional war, the accepted standard of what constitutes 'sufficient' certainty was undergoing a significant adjustment to meet an allegedly more uncertain reality.

Another key case in this trend was the emergence of drone warfare as a major player in military counter-terrorist operations. The Barack Obama administration (2009-2016) enthusiastically embraced drones – or, technically, unmanned aerial vehicles [UAV]. The language of a 'clean' war expressed the vision where hi-tech surveillance and its predictive knowledge production would erase enemy combatants – and only enemy combatants – before the messy and contagious violence of traditional warfare could begin (e.g. Gregory 2011; Singer 2009b). Of course, no technology is guaranteed an infallible claim to 'effectiveness', but rather must socially construct standards and measures like accuracy and precision (Gates 2011, p7, 48). Since the first confirmed use of UAVs in a 'kill operation', variously pegged as late 2001 or early 2002 (Sifton 2012; Woods 2015; also see Singer 2009a, p33-5), drone warfare has been dogged by public consternation over how this complex, human-nonhuman system (see Asaro 2013) 'knows' to kill. In a parallel to the state defense of NSA surveillance, the justification of drone strikes have often fallen back on secret proof and publicly unverifiable knowledge. What the

Snowden files show in this regard is the state's active production of the right numbers, the right categories, the right standards, that would allow the construction of sufficient certainty for each drone strike, and sufficient proof for its justification. Leaked files on drone operations in the Hindu Kush between May and September 2012 thus show a tendency to label unknown casualties as 'enemies killed in action' [EKIA]; the victims of drone strikes, eviscerated from afar, thus 'count' towards the justice of their own deaths until proven otherwise. Ultimately, the said operations – dubbed HAYMAKER – report 54 drone strikes yielding 157 EKIA, but only 19 'jackpots', or specific targets known to be dangerous (Devereaux 2015; also see Greenwald 2016). Often, the victims' basic demographic identity as "military-age males [MAM] in a strike zone" was sufficient to mark them for a speculative and deindividualised death (Becker & Shane 2012; also see Dasse & Kessler 2007, p420). Speaking about the case of Basaaly Moalin, Keith Alexander, then director of the NSA, explained the logic at work: to find the 'bad guys, "I need to know who his network of friends are, because chances are many of them are bad, too." (Schwartz 2015) Where Arab Muslims in the Middle East were fabricated into targets – and then killed – based on physical proximity, Arab Muslims in the United States were fabricated into threats, and sometimes arrested, based on communicative proximity. Across the

knowledge production work in drone warfare and sting operations, we find the same problem: the ethical consequences of a system of classification and a standard for sufficient proof (see Ananny 2016). The proliferation of subjunctive reason and its fabrication strategies legitimises an environment where being 'close enough', physically and metaphorically, is increasingly enough to count as guilty.

INTERPASSIVITY

> If the only people qualified to hold opinions are those who 'have all the facts,' then politics is not our responsibility. Politics is something that other people do, but not us […] The public exists elsewhere, not in our town, where regular people live (Eliasoph 1998, p134)
>
> We do not 'really' believe that politics may deliver everything it promises […] Nevertheless, as noticed, we do feel an intense connection to the political process and we do expect it to 'deliver' (Van Oenen 2006, p53-4).

If subjunctivity was about pulling in potentiality and the future to 'count' for the work of knowing, then interpassivity is about pulling in others, human and machinic, to fulfil some part of the knowing 'for me', 'in stead of me'. We have seen many aspects of this already in Chapter 1, though from a different conceptual vantage point. It is the NSA's Michael Hayden (2006), assuring the public that he absolutely trusts the NSA analysts with our personal information, and so we should his their trust in the NSA. It is Edward

Snowden, or Glenn Greenwald, the court, activists, or even the nonhuman documents, standing in for large sections of the public that lack access – practical or absolute – to the 'full information' for judgment. And it is even the idea of a general uproar over surveillance, the sense that 'the public' or 'American society' is working themselves up about it, that justice is being served (or worried that its 'national security' is being compromised). Interpassivity thus describes the modality of knowing proper to the distributed and recessive characters of knowledge production in the surveillance society.

Interpassivity originally arose from art and media theory as a converse to the cliché of interactivity, and then was developed as a theory for a wider range of social process primarily through the writings of Slavoj Žižek, Robert Pfaller and Gijs van Oenen (Pfaller 2003; Scholzel 2014; Van Oenen 2002). Though each articulation is distinct, they tend to revolve around one general relation: 'not me, but another for me'. Someone else believes, so that even if I do not, it remains a kind of 'truth' (Žižek n.d.). I Xerox a book or VCR a television show, and become satisfied that I have nearly consumed it – almost as if the machine has 'watched it for me' (Pfaller 2003). This subjective 'outsourcing' (Van Oenen 2002), has numerous practical uses. Interpassivity allows subjects

to 'know' that which may not be supported by their own behaviour, identity and environment in any immediate sense. This is the idea that 'I' may not believe in a conspiracy theory, but others do; that although I am not offended by a bad joke or violent footage, other people might.[80] In such cases, the interpassive articulation partially excuses the subject from being bound to the belief in question – even as that belief is hypostatised into assumed reality, thereby forming a concrete basis for opinions and actions. Indeed, "delegating one's beliefs [can make] them stronger than before" (Pfaller 2001, p37); the claims about states of affairs are externalised from the speaker's own experience, becoming more difficult to dismiss as a mere flight of fancy. We are familiar with this mechanism, of course, in the work of rumour. The conceit 'I have heard it said elsewhere' holds the truthfulness of the rumour in constant suspense, adding to its resilience. And such interpassive characterisations have been particularly important to mediated ideas of the public. The modern notion of the public has ever been predicated on the

[80] This aspect of interpassivity intersects with what communication literature more typically recognises as the third-person effect. The latter focuses specifically on the imagined impact of mass communications: i.e. the belief that violent rap music or sensational misinformation would affect a broad category of 'others' more than they do myself. Interpassivity, as I use it here, includes and goes beyond the third-person effect. Here, the other is not simply the gullible or otherwise weaker party, but often provides functions that the self or his/her immediate environment is incapable of fulfilling. Hence the other can 'know' in my stead, or politically participate for me – and the other can also include nonhuman actors, like technological objects or institutional systems.

ability to imagine silent majorities and other 'Others' behind each singular spokesperson or representation (see Hong 2014).

One *prima facie* reading of interpassivity is that it is a kind of divestment; a disempowering alienation of the subject from his/her own activity (including 'knowing'). Intersecting with contemporary critiques of participatory politics, Žižek calls interpassivity a form of 'false activity' where upper-middle-class academic may celebrate (or condemn, it matters not) the revolutions of others, and where the VCR will record the television show while the subject labours, *as if* rest and relaxation has been had (Žižek 1998, p6-7). Yet interpassivity is not simply a problem where the ceaseless activity of deputising machines masks the absence of the real thing. To be passive, and to have others do in one's stead, takes a different kind of work on the subject end. If digital activism is a mere simulation of real protest, and social media platforms a diluted form of meaningful sociability, the likes, retweets, emails constitute a kind of maintenance – the labour required to stay connected to others, intelligible as a public subject, countable as data (also see Matviyenko 2015)[81].

[81] Such 'maintenance work' is at a more general level than the problem of 'free labour' in the digital economy, where subjects are enrolled into unpaid, immaterial forms of work to support the allegedly free circulation of information and culture (e.g. Terranova 2000; Andrejevic 2010). Rather, I am referring to the ways in which allegedly 'passive' forms of consumption and public citizenship in new media societies nevertheless *occupy* us in

Interpassivity cannot be isolated onto a single side of the active/passive coin. Where Žižek and others tend to perceive the divestment of activity and the blooming of 'secondary' activity as duplicitious and disempowering, I focus on the ways in which interpassivity is leveraged as a mechanism for knowledge and meaning.

***

> Here's the rub: the instances where [NSA surveillance] has produced good – has disrupted plots, prevented terrorist attacks, is all classified, that's what's so hard about this.
>
> -Dianne Feinstein (in Knowlton 2013)

Such was the public defence raised by Dianne Feinstein, itself a part of a broader public relations effort by state actors in the wake of the Snowden leaks. Feinstein had been Chairman of the US State Select Committee on Intelligence (also called Senate Intelligence Committee), a major oversight body for state intelligence activities. This external auditor to the NSA's surveillance programs was now joining the fray to defend intelligence agencies' right to remain shielded from public oversight. The *form* of this

---

interpassive engagement, engagement that has been criticised as 'mindless frenetic activity' (Žižek 1998, p7). (also see Crary 2013; Han 2010)

apology is a simple one: if only you knew what we know, you would feel as we do – provided, of course, that you believe us that we even know anything. Of course, such appeals to the secret, the publicly unknown, is so often paired with a controlled leak, an open secret (Melley 2012). Even as one insists that the proof of surveillance's efficacy is secret, something about that secret is described, characterised, with impunity (literally, without the ability to be validated). Hence Feinstein was joined by General Keith Alexander, then Director of the NSA; Mike Rogers, a Republican senator and part of the House Intelligence Committee; and, presumably advised by them, President Barack Obama. All three insisted that a very specific number of fifty-four terrorist attacks had been thwarted, "saving real lives" (Elliott & Meyer 2013; Sterman 2014), as a result of the surveillance programs in question. As we have already seen, it was not long until Alexander and others had to backpedal to just one concrete case: the 2009 bombing plot by Najibullah Zazi (Clarke et al. 2013; Angwin 2014). Yet the idea that surveillance 'saves lives' continued to circulate in public debates; interpassive knowledge, like rumour, often develops a distributed and resilient network of veridical authority.

These kinds of claims do more than simply claim the public's ignorance of 'all the facts'. They also demand that public deliberation take place in full

awareness of that ignorance. Feinstein's apology asks the reading public to actively hold their judgment in abeyance. More than that, they ask that public knowledge is constructed by simulating the judgment, the affects, of another. Just a few weeks after Snowden's initial leaks, Keith Alexander made an appearance at Black Hat, a major information security conference well known for its hacker contingent. (The very name 'black hat' references hackers that attack secure systems, and although many conference attendees have traditionally been closer to 'white hat's working to protect such systems.) Undeterred by some skeptical and angry catcallers (O'Harrow Jr. 2013), Alexander pitched his appearance as a no-nonsense presentation of the facts, an occasion for setting the record straight:

> [NSA analysts'] reputation is tarnished because all the facts aren't on the table. But you can help us articulate the facts properly. I will answer every question to the fullest extent possible. And I promise you the truth (*LeakSource* 2013).

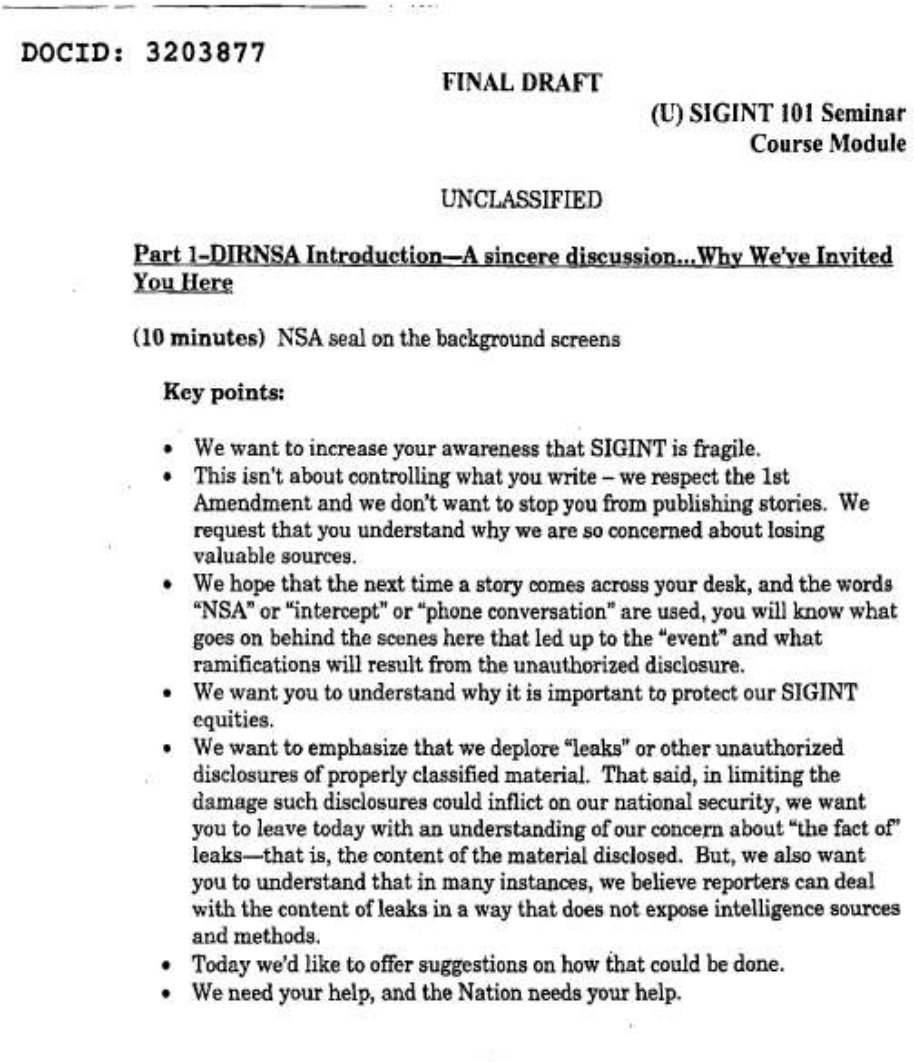
This promise, of course, was couched by repeated reminders that there are things that the audience cannot be told, and that some things would have to remain secret. This PR strategy was not new to the NSA; the organisation had already practiced similar rhetoric on its occasional briefings to journalists and

other outsiders (Fig.12).[82] Alexander's 'facts on the table' often consisted of tautological value judgments: he knows the analysts are great people, he knows that the NSA has great oversight – so those are the facts! In effect, the tech community gathered at Black Hat were being asked to become public advocates for the NSA's truth while being barred from full access to that truth themselves. The assertion that 'this is no bullshit' simulated the presence of facts and sought to produce an interpassive mode of verification.

A year later, little had changed in the demarcations of secret and public knowledge, open proof and simulated proof. In January 2014, the Senate Intelligence Committee – still chaired by Feinstein – held one of its annual open hearings. It was covered widely by the media, as well as being streamed online (*The Washington Post* 2014; *Senate Intelligence Committee* 2014). Feinstein now had occasion to lead the overseers' questioning of individuals like James Clapper. This hearing – a public affair that is nominally supposed to grant

[82] The NSA held 'SIGINT 101 Seminars' for journalists in the early 2000s. One 'course outline', first retrieved through a Freedom of Information Act by the *New York Sun* (Gerstein 2007), describes the NSA's stated objective as *not* "about controlling what you write", but that the journalists "leave today with an understanding of [the NSA's] concern about 'the fact of' leaks – that is, the content of the material disclosed" (*NSA* 2002). Here we find the same appeal to 'real facts' as opposed to leaked ones, and the request that journalists become convinced of the justice of surveillance while still being on the dark side of secrecy: "We need your help, and the Nation needs your help." The journalists were even presented with a school-like exercise to produce 'an innocuous rewrite' of a leak-based article about Osama bin Laden.

transparent access to the states of affairs and enable democratic deliberation – featured exchanges like the following:



DOCID: 3203877

FINAL DRAFT

(U) SIGINT 101 Seminar
Course Module

UNCLASSIFIED

Part 1–DIRNSA Introduction—A sincere discussion...Why We've Invited You Here

(10 minutes) NSA seal on the background screens

Key points:

- We want to increase your awareness that SIGINT is fragile.
- This isn't about controlling what you write – we respect the 1st Amendment and we don't want to stop you from publishing stories. We request that you understand why we are so concerned about losing valuable sources.
- We hope that the next time a story comes across your desk, and the words "NSA" or "intercept" or "phone conversation" are used, you will know what goes on behind the scenes here that led up to the "event" and what ramifications will result from the unauthorized disclosure.
- We want you to understand why it is important to protect our SIGINT equities.
- We want to emphasize that we deplore "leaks" or other unauthorized disclosures of properly classified material. That said, in limiting the damage such disclosures could inflict on our national security, we want you to leave today with an understanding of our concern about "the fact of" leaks—that is, the content of the material disclosed. But, we also want you to understand that in many instances, we believe reporters can deal with the content of leaks in a way that does not expose intelligence sources and methods.
- Today we'd like to offer suggestions on how that could be done.
- We need your help, and the Nation needs your help.

Figure 12. 'SIGINT 101'

Senator Heinrich: OK. Let me move on to Director Clapper and change gears a little bit to Edward Snowden. The revelations by Edward Snowden regarding U.S. intelligence collection have obviously caused some tensions with our European allies. Have our

	European allies ever collected intelligence against U.S. officials or business people, or those of other allied nations?
Director Clapper:	Yes, they have. I could go into more detail on that in a classified session.
Senator Heinrich:	That's fine, Director Clapper. Russia recently announced that it would extend Edward Snowden's asylum and not force him to leave their country. Do you believe that the Russians have gained access to the documents that Edward Snowden stole […] ?
Director Clapper:	I think this might be best left to a classified session and I don't want to do any – say or do anything that would jeopardize a current investigation.
Senator Heinrich:	That's fine, Director (*The Washington Post* 2014).

It is good that we have public hearings to tell us which particular things are not public! To be less glib: certainly, one can hardly expect nothing to be classified in even an open hearing on national security threats. Full transparency is an impossible ideal. Yet here, the public is not simply denied access to information; it is also exposed to a particular experience of deferral, one which again draws public attention to the secret beyond as the domain of truly consequential facts and evidence. All this was compounded by admissions that even the special court tasked to know in the public's stead – a court that is itself secret – also judges in ignorance. Reggie Walton, the presiding judge of the Foreign Intelligence Surveillance Court [FISC] at the time, explained:

> The FISC is forced to rely upon the accuracy of the information that is provided to the Court… the FISC does not have the capacity to investigate issues of noncompliance, and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders (Leonnig 2013).

The public is thus deprived of even the knowledge that the law or the government 'knows' in its stead. Rather, it is an indistinct other, dispersed and elusive, which guarantees the secret proof of surveillance's efficacy and justice. By brute forcing this kind of public scrutiny on the NSA, FISC and other branches of the American government, the Snowden leaks provoked a crisis of confidence not only in the state surveillance apparatus itself, but the interpassive relations governing its verification. In *An Inquiry into Modes of Existence* (2013), Bruno Latour recalls witnessing a 'shocking question' addressed to a climatologist at a conversation on climate change: "but why should we believe *you*, any more than the others?" The reply: "if people don't *trust the institutions of science,* we're in serious trouble." Latour suggests that this very answer reflects a fragility in such a trust; were the interpassive chain between Science (with a capital S), experts and the public secure, the climatologist could have confidently brushed off the question by virtue of a shared certainty in that epistemic relation (also see Beck 1992; Giddens 1990). Both climate change and surveillance / terrorism are what Timothy Morton (2013) calls *hyperobjects*: things which are too vast and unknown to be fully

accounted for by existing mechanisms for knowledge and, yet appear almost ubiquitously, in myriad individual instantiations. In such cases, the public is enjoined to 'know' a problem so distributed and remote that interpassive processes gain a special relevance. Yet it is precisely that interpassive process, that ability to trust in institutions and experts and specialised logic, which is challenged in both cases.

This state of affairs precedes individual subjects' decision to think this way or that about the insiders' claims. Even a cynical stance, which assumes that Feinstein and others are lying and there is no proof at all, requires some presumptive position to be taken against the knowledge that another has in one's stead. Similarly, to *abstain* from a firm opinion on the basis of insufficient knowledge can still leverage interpassive projections. Nina Eliasoph's ethnography of Americans' everyday discussion of politics describes communities which consistently shy away from talking politics. When Eliasoph herself brought such topics up, it was seen as 'an inert, distant, impersonal realm' too hard to get a handle on. It was a shame that political problems happened, and the 'public' should do something about it, they would say; but that 'public', the people who ostensibly knew enough to debate the problem, was invariably somebody else, somewhere else (Eliasoph

1998, p131-135). Even the refusal to have an opinion was qualified by the interpellation of an other who participates in publics in my stead. The recourse to interpassivity is not predetermined, but neither is it an entirely free choice. It is a responsivity provoked and encouraged by a situation – a situation consisting in this case of the recession of surveillance, including the logic of secrecy and security folded into the debate.

Not only can the other know for the subject, but they can also *do* and *experience* in one's stead. Since surveillance's pervasiveness far outstrips the highly infrequent occasions on which it intrudes tangibly into individual lives, interpassivity became a key technique by which a given political and affective orientation becomes fleshed out into 'known' reality. In the wake of the Snowden leaks, commentators often fell back on projected others – ignorant, outraged, afraid, and so on – to populate this verisimilitude. Consider one journalist's anecdotal example:

> My older, conservative neighbour quickly insisted that collecting this metadata thing she had heard about on Fox was necessary to protect her from all the terrorists out here in suburbia. She then vehemently disagreed that it was okay for President Obama to know whom she called and when, from where to where and for how long, or for him to know who those people called and when, and so forth (Van Buren 2013).

One might read this as typical liberal snarkiness about the cognitive dissonance of a stubborn conservative – intertwined with a certain patronising dismissal of the less educated. But the general sentiment that there are people out there, 'bad things' happening out there, that need to be watched and stopped is far from an abnormal one. The proliferation of interpassive relations in surveillance discourse thus enables the neighbour's imaginations of her own safety or danger to emerge from a situation where someone else is surveilling someone else. When interpassively simulated claims are presented as knowledge, the judgment and action that follows from it also becomes amenable to such deferral.

As with subjunctivity, the pattern was replicated on the other side of the debate. For many critics of surveillance, Edward Snowden, the heroic truth-teller, and his media proxies – primarily Glenn Greenwald and Laura Poitras – formed the authoritative others who might 'know' in their stead. We have already considered in Chapter 1 how, faced with the sheer flood of technically available information, it was often a necessary strategy to defer to such situational experts to read, understand, interpret in the public's stead. Figuratively speaking, we've all xeroxed those top secret memos; most of us will probably never touch them again, but there they are, glowing in their

potential ability-to-inform. A probably unintended gesture to Snowden's interpassive function appears in the final scenes of *Citizenfour*, Laura Poitras' Academy Award-winning documentary on the leaks. Having released his cache of secret files to the world, Snowden has fled the Hong Kong hotel where it all began and found asylum in Russia. In the scene, he is visited by Glenn Greenwald, who would like to update Snowden on a new source, a new whistleblower. Possibly as a precaution against eavesdropping, Greenwald scribbles every critical term – the source's name, their means of communication – on a piece of paper. The audience is denied this key information even as Greenwald and Snowden discuss the revelations on camera. A New Yorker review, christening Snowden the 'Holder of Secrets', was not happy with this choice:

> Several times, Snowden reacts to disclosures that we are not allowed to see; it's as if the viewer were supposed to accept his judgment literally at face value. Poitras has closed a curtain around her main characters, leaving the audience out (Packer 2014).

As a criticism of the scene itself, this is vacuous; the film has a clear moral obligation to protect the identity of this new whistleblower. But the complaint illustrates the relationship that has been established between Snowden the truth-teller, the public upon whom he wishes transparency, and the truth

itself. The business of revealing secrets must be a secret affair, in exactly the same sense that surveillance must itself operate in the dark while hoarding and trading in the unknown. The secret's incitement to discourse (Foucault 1998), and the constant need to characterise and operationalise the secret and the unknown, is mirrored across both 'sides' of the Affair. In fact, within the small community of whistleblowers on 21st century American state surveillance, Snowden should be considered unusually frank: other publicly named figures, such as former State Department official John Napier Tye, consistently fell back on a interpassive relation where the whistleblower must know and the public must simulate.

> 'Based in part on classified facts that I am prohibited by law from publishing,' Tye wrote, 'I believe that Americans should be even more concerned about the collection and storage of their communications under Executive Order 12333 than under Section 215.' I wonder what he saw but isn't revealing (Friedersdorf 2014).

Similarly, if on the state side judicial bodies like FISC were forced to rule on surveillance's legality through interpassively acquired information, those contesting that legality from the civil society side faced the same problem. As we saw in Chapter 1, an earlier set of revelations on domestic phone call records collection had spurred a coalition of civil society organisations and

individuals to seek legal injunction against the NSA. One case clearly anticipated the state's argument for secrecy:

> Defendants argue that the state secrets privilege bars Plaintiffs' claims because Plaintiffs cannot establish standing or a prima facie case for any of their claims without the use of state secrets. Further, Defendants argue that they cannot defend this case without revealing state secrets. (*ACLU v. NSA* 2007, p.3)

This strategy was replicated in other legal challenges brought against US state surveillance in this period; for instance, *Jewel v. NSA* (2008), led by the Electronic Frontier Foundation, saw the NSA make an identical attempt to have the claims dismissed. Of course, it is unlikely that the 'full' facts of intelligence activity and surveillance procedures could ever be articulated publicly. The practical impossibility of eliminating secrecy from public knowledge and transparency thus resembles, and collaborates with, the persistent presence of uncertainty and the unknown in surveillance as an epistemic problem.

***

The other that knows, does, decides, for the subject… this other is not limited to human individuals, or even aggregates of individuals, but extend to the

machinic. Dianne Feinstein defended the mass, automated collection of communications data with an apparently self-explanatory quip: "Part of our obligation is keeping Americans safe … Human intelligence isn't going to do it." (Bohan 2013) It *was* self-explanatory to a particular community, at least. Feinstein was referring to a widespread classification within the intelligence community between HUMINT [human intelligence] and SIGINT [signals intelligence]: between the human business of managing individual sources, and the scalable, automatable, machine-dominated collection of electronic communications signals. While the classification can be more variegated (for example, GEOINT, the use of geospatial data, and OSINT, the collection of publicly available information), the balance of emphasis between human sources and intercepted electronic signals has been a major narrative frame within the intelligence community[83] and in popular cultural representations. Thus a NSA strategy statement in 2012, leaked by Edward Snowden, references the present as a 'golden age of SIGINT' (Risen & Poitras 2013). In such articulations, SIGINT is the inevitable protagonist to the age of the

[83] The Snowden files show that the NSA was bullish in pushing SIGINT as "*THE decisive edge*" for US national security in the Internet age, and indeed claims a 'golden age' of SIGINT (Risen & Poitras 2013; *The New York Times* 2013). Of course, the NSA in particular has been a leading player in SIGINT for decades (Laprise 2016). However, the NSA's success in achieving a drastic increase in funding and prominence after September 11 – which we narrated in Chapter 1 – has been a part of a renewed emphasis in the powers of SIGINT. Other examples of this narrative include (*The Economist* 2015; Margolis 2013). Snowden himself has framed his criticism as the problem of overrating SIGINT programs "that do not work" at the expense of HUMINT (Snowden 2016; also see Silverstein 2015).

Internet and global communications infrastructures, a necessary shift dictated by the flow of history. The narrative of SIGINT's necessity thus forms a certain parallel with self-surveillance's vision of automated and autonomous data collection. Both interpellate a world of knowing machines that can produce *meaningful* knowledge prior to or in excess of human intervention.

Machines that know in our stead loomed even larger in the explicitly fictional and hypothetical. Interpassivity does not stop at projecting what is known by others or realised in secret, but also leverages more speculative literature to render intelligible reality that is so often occluded by secrecy and uncertainty. Although the vast majority of the NSA's SIGINT activities, down to the names and existence of programs like PRISM, have been top secret, there is also a long tradition of intentional leakages to the public via 'strategic fictions', penned by literature students and writers in the CIA's employ (Melley 2012). Literature from DeLillo to Burroughs and Pynchon, and Hollywood films like *Enemy of the State* (1998) and *Echelon Conspiracy* (2009) have acted as sites to play with ideas of reality. In other words, they are platform for thinking through surveillance if not as a presently deployed set of practices, then a set of principles, power relations, technical paradigms, that flit between merely plausible and believably probable. Indeed, when Snowden first began to leak

government secrets, one of the first points of reference for the media and the public was George Orwell. A few months after his flight from Hong Kong, Snowden himself saw fit to reference the writer:

> Great Britain's George Orwell warned us of the danger of this kind of information. The types of collection in the book – microphones and video cameras, TVs that watch us – are nothing compared to what we have available today. We have sensors in our pockets that track us everywhere we go. (Snowden 2013)

Yet the comparison was rather redundant. Sales of Orwell's *1984* had already rocketed by some 6,000% after his initial leaks in June (Hendrix 2013). Of course, one cannot claim that the public flocked to Orwell, Dick and Huxley in order to take them literally as prophecy. But such fictional work clearly served as resources for making sense of the confused present and the uncertain future; Aldous Huxley's *Brave New World,* and Philip K. Dick's *The Minority Report* (or, more often, the Steven Spielberg film adaptation) became staple references for communicating the just-unveiled reality of state surveillance (e.g. Burris 2016; Greenwald 2014a). Indeed, in some cases, such writings were explicitly understood by their creators as fiction which combats the deception of the state: that is, fiction is a work of 'true lies' which finds its own ground to resist the lies that roam dressed as fact (Melley 2012, p115). Meanwhile, state actors, also participated in this detour through fiction; in

March 2014, the high-profile TED Conference invited Snowden and the NSA to speak in succession, and the latter's defence included an uncanny reprisal of the technological fantasy in *The Minority Report*:

> If you think about a television murder mystery, they start with the body and work to solve crime. We're starting well before then, before the bodies, to figure out who the people are and what they're trying to do. That involves a massive amount of information (Ledgett 2014).

The machines that know for humans, and machines that know beyond what humans can know: both run amok in this speculative space, fleshing out the skeletal outline featured in more 'serious' and prudent discussions of the Snowden files. The narrative of historical shift from HUMINT to SIGINT received its doppelgänger in popular cinema of the 2010s: in *Spectre* (2015), James Bond, that archetypical hero of face-to-face spy work, is threatened not by Soviet-affiliated agents (as he was in *Dr. No* (1962) or *From Russia With Love* (1963)), nuclear weaponry (as in *Thunderball* (1965) and *Octopussy* (1983)) or even nation-specific, organised terrorism (*Casino Royale* (2006)), but an ubiquitous surveillance system coordinated across nine national members of the 'Nine Eyes' – an obvious derivation of the real-life 'Five Eyes' alliance that has evolved since 2001 to extensive surveillance cooperation. Sherlock Holmes, the figure which exemplified a pre-digital sensitivity towards

physical traces and surveillance through human sensory equipment, was reprised as a contemporary detective in a highly successful BBC series (*Sherlock*, 2010-). There, as Cory Doctorow (2016) points out, Holmes remains the arrogant and mercurial master of HUMINT, but clearly contrasted by his brother Mycroft that functions as a superhuman clearing house for a vast web of SIGINT. And while Holmes may be the hero of that story, it is made perfectly clear that Mycroft and SIGINT are the domains through which everything of political and governmental consequence is run. Even the American superhero genre has yielded *Captain America: The Winter Soldier* (2014), a film which consciously worked in a critical depiction of pre-emptive strikes as determined by data-mining algorithms (see Lovece 2014).

These fictions provided speculative spaces for public engagement with realities that often remained too secret and too uncertain to otherwise attain a firm grasp of. And if the cultural industries were simply reacting to political controversies in a bid to render themselves topical, they were also capable of *presaging* the Snowden leaks in the public consciousness. It has been argued that Hollywood has 'softened' the public up for the shock of 21st century electronic surveillance for years (Patterson 2013), such that the cliché 'we knew already' references fictional 'play' as much as serious investigative

journalism. Most directly, the US television show *Person of Interest* has been credited as the 'TV show that predicted Edward Snowden' (Rothman 2014). The popular US series presented the public with 'the Machine' – an NSA-style dragnet which 'spies on you every hour of every day', and which the protagonist would use to track down individuals before they became perpetrators or victims of violent crime. *Person of Interest*'s prophetic powers had rather mundane sources: the series was conceived through extensive consultation of U.S. state surveillance practices as was known and estimated at the time (Gan 2013). If the Machine is not quite an 'accurate' picture of the present day capacities of NSA surveillance systems, the vision of 'connecting the dots', of predicting crimes before they happen, of profiling individuals based on populational patterns, are all played out in *Person of Interest*'s dramatic scenarios. In other words, the technically available information about state surveillance was percolating as much through fiction as news – a circulatory context which favours the fermentation of 'half-legitimate' epistemic techniques like interpassivity and subjunctivity.

Some of this imaginative media also intersected the contemporary surveillance debate with an older tradition of representing crime and police work. On one hand, 'The Machine', *Person of Interest*'s mass surveillance

program, is clearly based on and evocative of U.S. state surveillance, providing the public with a simulation of hypotheticals. On the other hand, the show crafts a verisimilitude where urban crime of every kind proliferates and may strike *any* individual without notice. Cultivation theory (Gerbner et al. 1980; also see Romer & Jamieson 2014) suggests that media can have long-term, sedimented effects – that it can train people into presuming phenomena that lie beyond their own lives in order to, say, develop a heightened fear of criminal victimisation. This is not to say that *Person of Interest* is alarmist. The point is that insofar as terror and crime are not everyday realities for many (not all) of the population, fiction becomes a key supporting resource in the ongoing efforts to close the epistemic gap.

ZERO-DEGREE RISK

Catalysed by September 11, early twenty-first century America – its politicians, its media, its public – affixed terrorism as a powerful presence in its social imaginary. During the Snowden Affair, some voices cautioned that all this might have been blown a little out of proportion; after all, the actual chance of dying from a terrorist attack in America was 1 in 20 million between 2007 and 2011 (Barrett 2013). Barack Obama was known for assuring both the public and his own staff that "the odds of people dying in a terrorist attack,

obviously, are still a lot lower in a car accident" (Vickers & Leno 2013), or even falls in bathtubs (Goldberg 2016). Indeed, as *The Washington Post* pointed out, "you're more likely to be fatally crushed by furniture than killed by a terrorist" (Shaver 2015). Yet the invocation of such statistics (which hardly dampened the discourse) illustrates the troubled relationship between surveillance, terrorism, and statistical or probabilistic knowledge. On one hand, what knowledge can statistics deliver about an event like September 11, a devastation of a singular significance in the context of American history – or a figure like the lone wolf terrorist, a figure that hides in the many residuals left by quantified demographics? On the other hand, the play of correlations and probabilities *is* precisely how data-driven surveillance promises to render such events predictable and preventable – and, even, how the benefits and harms of such surveillance are assessed . The impossibility of statistical risk calculation is intertwined with a renewed vision of total calculability.

This tension consistently broke out into public discourse over the course of the Snowden Affair. We saw one aspect of this tension in Chapter 1: a fascination with numerical representation as a way to grasp the distribution of knowns and unknowns vis-à-vis surveillance. More pointedly, the question of terrorism's probability – and the calculation of surveillance's effectiveness –

became a key site for claiming and contesting the legitimacy of surveillance practices. An overarching frame was furnished by the frequently expressed notion that the problem of surveillance is to find the right 'balance', to strike the right 'bargain', between the conflicting values of security and privacy. Soon after September 11, in a statement to the US Congress (and available to the public), NSA Director Michael Hayden insisted on this framing:

> What I really need you to do is talk to your constituents and find out where the American people want that line between security and liberty to be […] We need to get it right. We have to find the right balance between protecting our security and protecting our liberty. If we fail in this effort by drawing the line in the wrong place […] the terrorists win and liberty loses in either case (Hayden 2002).

He would repeat the idea of 'balance' repeatedly – to the National Press Club as a Deputy Director of National Intelligence (2006), and later in his autobiography as a retired general (2016). Barack Obama's defence of surveillance programs also invoked a similar bargain:

> But I think it's important for everybody to understand, and I think the American people understand, that there are some trade-offs involved […] And the modest encroachments on privacy that are involved in getting phone numbers or duration without a name attached and not looking at content – that on, you know, net, it was worth us doing (Obama 2013).

The idea of a grand 'bargain' asks the public to weigh the pros and cons of state surveillance, and to balance the equation towards a Goldilocks point where harms might be minimalised and benefits maximised. It is a classic case of risk-oriented, actuarial thinking. Yet efforts to deliberate towards this balance expose a deeper epistemic problem: how can surveillance be 'balanced' if its effects cannot be assessed in meaningfully quantifiable terms? What kinds of statistical reasoning and risk calculus can be enacted, with surveillance and with terrorism, when it involves the collection of literally uncountable pieces of data with the aim of preventing even a single attack (under the full awareness that absolute security is impossible)? Consider contemporary efforts to ascertain the value of surveillance. As we have already mentioned, only a *single* case – of Basaaly Moalin – is publicly available to prove, exemplify, or otherwise indicate surveillance's performance with respect to the terrorist threat writ large. The imbalance of numbers struck numerous contemporary observers. The *New Yorker* asked:

> the N.S.A. has [collected] records from hundreds of billions of domestic phone calls […] the government has not shown any instance besides Moalin's in which the law's metadata provision has directly led to a conviction in a terrorism case. Is it worth it? (Schwartz 2015)

The question reveals the powerlessness of numerical estimations when the objective is supposed to be absolute prevention. This tension between 'zero tolerance' and the probabilistic nature of modern risk can be found across other counter-terrorist efforts. Harvey Molotch (2012) describes a multi-million dollar surveillance system installed in New York's subways over the mid-2000s, a project where the political demands for concrete action overcame the transport authority's own skepticism. As of 2012, the system had yielded a small number of arrests for misdemeanours, and not a single lead related to terrorism; in other words, its 'cost' in the form of money and civil rights had yielded no tangible 'benefits'. Meanwhile, actors continued to manipulate numbers and statistics as a way to shape the epistemic field. '1944 New Yorkers saw something and said something', insisted an iconic poster produced by the transport authority, though the number has yet to be traced to any actual documentation (Molotch 2012, p54). Yet the point of a subjunctive knowledge environment is that the absence of proof does not authorise certainty one way or the other; after all, unknown terrorists may have been deterred from attempting terrorist attacks by the presence of cameras. Or the system may yet live to catch a terrorist red-handed – if not tomorrow, then next month, next year… Andrew Liepman, who had been Director of the National Counter-Terrorism Centre from 2005 to 2012,

described the political climate in that period as a "zero failure, zero attack threshold" (Barker 2016; also see Aradau & van Munster 2007, Cooper 2006). As we saw with strategies for fabrication, terrorism had become an epistemic problem not so much concerned with minimising probabilities and constructing acceptable models of risk, but a politically charged search for absolute certainty in a context where a degree of unknowability is inherent. In this formulation, the benefits of a surveillance system remain formally unfalsifiable precisely because no calculation of 'bargain' or 'balance' between security and privacy can be properly achieved.

The efforts to understand surveillance and terrorism in terms of risks, probabilities and cost/benefit analyses produced an air of calculability, but in practice reinforced the dilemmas of trying to know the unknowable – whether that be the risk of terrorism, the preventive benefits of surveillance, or even its harms. Like subjunctivity and interpassivity, we find a practical heuristic which does not seek to erase the presence of uncertainties, but leverages them as a way to justify and operationalise its claim to sufficient knowledge and certainty. We can schematise and situate this heuristic more appropriately by examining its relationship with more 'orthodox' understandings of risk.

***

Before September 11 had hyper-charged surveillance with political relevance, theories of risk had already begun to respond to what it saw as new trends – emerging gradually over the 80s and 90s – towards more extreme, and less knowable, kinds of risks. At this point, the emblematic figure was climate change: global, long-term, both too dispersed or micro-level and too enormous to calculate adequately. In response to such dangers, major figures in risk studies, like François Ewald (1993) and Ulrich Beck (2009), developed a historical narrative about the rise of 'catastrophic' and otherwise exceptional risks: dangers which lie outside orthodox risk calculability, or even a society's ability to know in general (O'Malley 2004). In his seminal best-seller *Risk Society* (1992, the original German published in 1986) Beck had depicted a modern attitude to risk defined by its establishment of a rigorous *economy*: a system of 'acceptable levels' (that is, acceptable failures, deaths, disasters) that colonises successive real-world problems as 'known risks' and thereby imposes a clear grid for calculating optimal decisions and practices. By 2009, near the end of his life, Beck (2009) was now arguing that societies are experiencing a swell of unknowns and unknowables, and that responses to climate change and terrorism characterise a 'planetary state of exception' to

the rule of risk calculability. As Dean (1998) and others point out, however, there is no firm proof of any quantitative or qualitative change in the dangerousness of our world in realist terms. In any case, risk has always been a question of how dangers are perceived and calculated by societies – and it is in this epistemic sense that the differences must be counted.

In this regard, it is important to remember that risk in the former, classical sense itself developed out of a proliferation of data and widespread enthusiasm about its epistemic capacity. As "the world teemed with frequencies", as Ian Hacking (1990, p97) put it, scholars of the 19th century (and some predecessors, like Condorcet and the 'moral scientists' in the 18th) rushed to establish laws and models that could leverage the new availability of data to produce new knowns and certainties. In an echo of contemporary pursuits for statistical predictors of lone wolf terrorists, this heyday of modern risk included both the expansion of actuarial calculations like predictors for sickness and efforts to identify 'criminal' faces or 'inferior' skull shapes (Sekula 1986, Gould 1996). Such rationalising work often swept away (though not completely) many older heuristics for danger, luck and chance (Lears 2003), but this conquest was itself achieved through a host of often arbitrary decisions. Hacking (1990) relates a striking example in the 1820s: the

British parliament, eager to establish actuarial laws to facilitate life insurance businesses, was challenged by John Finlaison that such a law was not calculable at the time. Finlaison, the first president of the Institute of Actuaries, had been summoned by MPs as an expert on the matter. Rather than heed his expertise, however, they cajoled and bullied Finlaison repeatedly until the man grudgingly produced some numbers. The normalisation of risk logic itself involved a set of heuristics and veridical objects for rationalising unknowns into knowns (or rather, probabilities). Early twenty-first century surveillance debates continued to invoke those high modern techniques – the language of statistics, probabilities, tradeoffs, equations – even as it threatened to unravel their promise of calculable 'economies'.

The heuristics involved in the Snowden Affair thus might be described as a 'zero-degree risk': a mode of knowing which intersects a veneer of statistical reasoning with a certain threshold of indeterminacy and negligibility, and defaults to a more speculative and pre-emptive kind of claim-making. Insofar as terrorist threat is conceptualised as a zero-tolerance event of incalculable harm, it defies mathematical calculations of value. If the risk of death from terrorism is lower than from a car crash, how low does it have to be to fall

under 'acceptable levels'? If a given surveillance program violates the rights of several million citizens to catch a single terrorist (or, as is often more likely, pre-emptively apprehend a suspect), is it 'worth it'? Instead of financial trading or gambling, where a certain ineliminable degree of uncertainty is accepted as the price for the benefits of risk and probabilistic reasoning[84], the post-September 11 climate espoused the fantasy of total security and total pre-emption. When the 'what if' side of the equation is as catastrophic as September 11, the 'value' that each rights violation holds on the opposite side of the equation doesn't just decrease: it becomes unquantifiable. This is not to say that surveillance and New Terrorism is entirely 'post-risk'. Actuarial reason might still declare a certain individual to be 'worth' a certain monetary premium, and the 2002 Terrorism Risk Insurance Act indeed incentivised insurers to provide packages for terrorism (also see Aradau & van Munster 2007). The effort to classify and predict the lone wolf, as witnessed in Chapter 1, demonstrates the enduring attraction of correlational and probabilistic calculations of risk – if not its successes. Zero-degree risk expresses the ways

[84] In other words, to be able to rely on risk as knowledge is to be able to live on as if the risk, sufficiently mitigated, simply did not exist. Thus we find, in the financial sector, the idea that subjects who thrive are those who are able to routinise and 'handle' risk, by which it is meant some subjective ability to 'sleep with it at night' (Martin 2002, p121). Another relatively extreme – and thus explicit – case is gambling: Schüll's ethnography of Vegas' machine gambling sees the industry speak of players "reclining on a math model" – a *comfortable* level of trust in calculable probabilities (2015, p109).

in which surveillance and terrorism – in public debate as much as its internal operations – struggle to establish a calculative reason, or at least a performance of such reason, over the incalculable. As a heuristic, its proliferation reflects the fact that even as the vision of data-driven predictivity and total archives articulates surveillance's ideal form, both its practitioners and the public are faced with the practical need to make decisions and assessments.

But if the instruments of calculative rationality are applied on material marked out as noncalculable, how is knowledge, certainty, to be established? In the Snowden Affair, and early twenty-first century debates over surveillance and terrorism in America more generally, the solution that emerged more or less took the sword to the Gordian knot: doing *something* must be better than doing nothing, and therefore 'everything' that can be done must be done. Matthew Hannah (2010) calls it 'actionism' – an intensification of a propensity for action and the performance of being 'proactive' that is latent to modern politics (Schneier 2013; Moeckli 2008, p40). One oft-cited instance is UK Prime Minister Tony Blair's defense of the American invasion of Iraq, itself very much tied to the political fascination with terrorist threats in this period:

> But sit in my seat. Here is the intelligence. Here is the advice. Do you ignore it? But, of course intelligence is precisely that: intelligence. It is not hard fact. It has its limitations. On each occasion the most careful judgement has to be made taking account of everything we know and the best assessment and advice available. But in making that judgement, would you prefer us to act, even if it turns out to be wrong? Or not to act and hope it's OK? And suppose we don't act and the intelligence turns out to be right, how forgiving will people be? (Blair, 2004; also see Aradau & van Munster 2007, p105)

Here, we might usefully recall Philip Mudd's words when he, from the position of a counter-terrorism specialist, explained to the families of a fabricated terrorist why such engineering of proof was necessary:

> People like me are in a difficult position. We cannot afford to let dozens of innocent people die because a youth makes a mistake […] If we switched roles, what would you do? What would you do? Would you let him go? (Barker 2016)

The logic has been employed to justify everything from CCTVs in schools (Taylor 2013, p19) to counter-terrorism in general (Schneier 2013). And of course, the NSA's post-September 11 strategy – to collect everything because anything might be important – is itself the clearest manifestation of actionism. The great contradiction between an absolutist, 'zero tolerance' politics and an uncertain world of 'catastrophic risks' is navigated through an ethics where one always opt to do, to save, to record, to arrest; an epistemology where the

known harms, or 'side effects', of surveillance is counted for less than the unknown harms of inaction (Daase & Kessler 2007). Beyond operational principles and specific legal cases, such a strategy also structures the public debate between privacy and security. As we have discussed previously, the problem of 'balancing' privacy has been a major frame for the Snowden Affair (e.g. Greenwald 2014b; Rusbridger et al. 2015) – even as it was frequently written off as 'already lost' and 'old-fashioned' (Yaverbaum 2014; Cohen 2013). What was notable about the challenges to privacy in this debate was the extent to which they demanded a more traditional epistemology. Legal arguments insisting that privacy advocates prove 'specific harm' caused by surveillance – which we saw in Chapter 1 – requires of privacy a certain standard of proof that arguments for security have already excused themselves from. Similarly, the popular refrain that those who have 'nothing to hide' are safe from surveillance (e.g. Marlinspike 2013)[85] misses the fabricated and anticipatory character of danger identification in the age of New Terrorism. Privacy's struggles to assert itself as an important virtue in the Snowden Affair exemplifies how thresholds for what counts as sufficient

[85] The 'nothing to hide' argument, in fact, has been more prominently aired by the *critics* of surveillance than its defenders. As we see with David Sirota earlier in this chapter, privacy advocates have tended to characterise or anticipate the public as needing to be educated out of such reasoning. Nevertheless, it is clear enough that state spokespersons make implicit references, typically by arguing that 'ordinary Americans' have nothing to fear from surveillance.

proof, sufficient knowledge, are being recalibrated in favour of an actionist and prescriptive strategy.

Actionism completes the zero-degree equation, and rationalises a pathway from uncertain epistemology to concrete decisions. Here, the *possibility* of future harms is prioritised over (or rather, enters in place of) *probability*, completing the irony of the mathematical veneer; it is precisely the things that escape statistical knowability that are presented as a firm basis for 'knowing enough' to act. In this sense, the fictional scenario of *Person of Interest* plays out a fantasy already embedded in the real world aspirations for total surveillance and prediction. In the television show, the Machine doesn't spit out correlations, simulations, probabilities; it simply provides, with absolute predictive certainty, the social security number belonging to the next victim or assailant. Alongside the practical strategies of fabrication, the invocations of zero-degree risk, and the actionist injunctions they are made to justify, the unerring tick-tock of the fictional Machine illustrates the actors' relentless quest for sufficient knowledge, sufficient certainty.

JUST-IN-CASE POLITICS

This array of heuristics for simulated and 'sufficient' forms of knowledge produces a specific epistemic terrain for more practical and directly politicised debates around the notions of privacy, of security, of freedom, of civil rights. Publicly presented as *realistic and necessary* instruments for the uncertain world of New Terrorism and dragnet surveillance, these heuristics legitimate and normalise an epistemic sensibility that largely maintains the official regime of rational and evidence-based reasoning, even as it provides ways for subjects to mobilise the uncertain and unknown for their public use of reason.

It would not be difficult to condemn these heuristics for 'cheating' the principles of open and rational knowledge production. Yet such criticism would miss the practical exigencies of their context. Although I cannot agree with more realist conceptions of risk that say the world has become a more 'risky' place than before, both surveillance and terrorism in the early twenty-first century do produce a collective imaginary of a highly uncertain and speculative threat – for both insiders and outsiders, practitioners and the lay public. Mark Andrejevic and Brian Massumi have both identified, in the George W. Bush administration (2001-2008)'s counter-terrorist strategies, a

significant step towards this willingness to pre-empt the facts, to move on 'sufficient' knowledge and to establish proof post facto. As Karl Rove, one of Bush's key advisors, pointed out:

> We're an empire now, and when we act, we create our own reality. And while you're studying that reality… we'll act again, creating other new realities, which you can study too, and that's how things will sort out (Rove *in* Andrejevic 2013, p16-7).

But this is not, as some have called it, a 'post-truth politics'[86], a politics that does not care about the truth or is willing to throw away the last vestiges of honesty. It is rather the development of a certain pragmatism, a rebalancing of what is considered necessary in the face of enduring uncertainties in a data-saturated world. If Andrejevic and Massumi identify an affective turn towards a more dismissive relationship with facts, what I have sought to emphasise is the changing rules within the epistemic schema itself. And that change concerns evolving thresholds of what counts as 'sufficiently' known; what kinds of unknowns can still be *used* for consensus, action, decision; how 'rational choices' are salvaged and cobbled together, even in the face of lone wolves and ubiquitous dragnets.

---

[86] James Fallows, writing for *The Atlantic*, has given this term some traction throughout the 2000s and 2010s (see Fallows n.d.; also Lepore 2016).

4. Honeymoon Objectivity.

In 2014, then-22 year old entrepreneur James Proud successfully crowdfunded a sleep sensing device that would automatically monitor sleep patterns, provide a numerical score, and make recommendations. It did not escape Proud that such functions were already available. Beddit, the sleep sensor with which we began Chapter 2, had itself been crowdfunded a year before, and was already released to its backers. Proud chose to emphasise his device's 'simple, uncomplicated and useful' qualities; he insisted that what matters is not technology that constantly reminds us to its technicity, but technology embedded into the everyday flow of attention and reflection.

Figure 13. The 'forgotten' sensor.

> With the rise of wearables, we've seen that people clearly care about their sleep. But to us, it felt so unnatural to be worrying about putting something on, charging it […] we believe technology needs to disappear […] everything in [our device] is just designed to fade away (*Hello* 2014).

It is fitting that Proud should have named his device in a similarly naturalising fashion: *Sense.* It joins Sentio, makers of the 'Feel' wristband which surveils bio-feedback and alerts users recommending that they smile, laugh, and otherwise manage their emotions; Sen.se, the makers of the home monitoring system Mother that we examined in Chapter 2; and more besides. And it is also fitting that, ultimately, a small sphere fitted with several basic sensors[87] and algorithms did not quite live up to either the fantasy of total seamlessness or the ideal of eliminating uncertainty in self-knowledge. While no sales figures are available, the Sense orb was panned by *The New York Times* (Manjoo 2015)*:* the device may 'work well enough, for what it is', but it was condemned as part of a 'little bit bogus' genre of devices whose 'reality come nowhere close to the promise'. Other media outlets, too, such as *Fast Company* (Barol 2015), were lukewarm; often, the rhetorical objective of new technologies were easier to support than their faltering, still immature

[87] In this case, Sense advertised sensors for humidity, temperature, ambient light, noise (microphone), air particles, and acceleration.

implementations. Even as a specific sensing device might spill out garbled data, hopelessly ignorant of the snoring Labrador in the bedroom or the tossing and turning of the human partner in bed, self-tracking discourse projects a near future where machinic sensibility can be melded into the very sensory rhythms of user-subjects. This chapter critically examines this discourse of data-augmented sensibility – a rhetoric which I label *data-sense.*

***

In previous chapters, we examined the ways in which claims of data-driven knowledge are consistently founded on the invocation of uncertainties (Chapters 1, 2). The veridical authority of data and surveillance-machines was asserted not only through the virtues like automation and intimacy (2), but a host of deferred and simulated practices of knowing (3). This relationship between knowledge and uncertainty was replicated even where surveillance technology was subject to criticism or breakdown – ranging from the incalculable thresholds of numbers and statistics (1, 3) to the 'humanistic' scepticism over machinic sensibility. (2)

This chapter picks back up the case of self-surveillance (2), as well as the question of how technological discourse seeks to reorganise what 'counts' as knowledge, or what is privileged as more 'accurately' true, that we had asked of state surveillance, terrorism and criminal intent (3). In Chapter 2, we saw how the promises of 'better' self-knowledge through automation and intimacy hinged on a certain binary: human intuition and experience as subjective and flawed, and quantitative, machinic sensibility as a privileged lens into objective reality. This chapter turns to the kinds of subjects and subjective qualities that self-tracking discourses projects as necessary and desirable for those developments in machinic sensibility. The human body, after all, is the 'first instrument' (Marcel Mauss *in* Peters 2015, p80-1); the medium which we inevitably mould whenever we reshape external objects into technological solutions. To lend this process legitimacy, self-tracking discourse specifically co-opted a broader, older modernist fantasy of objective knowledge and technological progress. Yet, as we will see, it is no coincidence that the way in which subjects are encouraged to adapt themselves to take advantage of new technological possibilities are exactly the way in which they are being made into voluntary producers of personal information for the new data economy – just as surely as the imperative of national security seeks to

routinise the subjection of American citizens into persistent and indiscriminate invasions of data privacy.

Data-sense, then, the label I use to identify a subset of self-tracking discourse: a rhetoric, which urges the necessity and inevitability of user-subjects that internalise data-driven modes of self-knowledge and privilege machinic sensibility as a route to self-knowledge. I have picked data-sense out from a set of similar terms and slogans used in self-tracking discourse – playing, in particular, on practitioners' frequent discussions of 'new sensors and new senses' (e.g. Lai & Forzani 2015). Primarily advanced by prominent thought leaders in self-tracking industry and the Quantified Self movement, this futurist rhetoric knitted together existing products, experimental solutions and futuristic prognoses into a mélange of rationalist, posthumanist, evolutionary ideals about how humans will and should learn to know themselves through machines. If machinic sensibility describes smart sensors' much-vaunted ability to collect data that humans cannot, data-sense describes the ways in which humans are to be instructed to become interfaces and clearing houses for that data – and thus become digital natives of a self-

tracking, data-driven society.[88] Here, our use of 'sense' draws upon both Merleau-Ponty's *sens* (meaning, sense, direction) and *le sentir* (sometimes translated as 'sense experience', involving 'to sense' and 'to feel'), and indeed, the double meaning of 'sense' still latent in everyday English: a sense for feeling, and a sense for making meaningful.[89] Data-sense describes the ways in which human subjects' sensory access to their own bodies, and their equipment for making sense of the data at hand, are both reconfigured – rendering them suitable systems for the production of self-tracking knowledge.[90]

This discourse thus forms the subjective half of the vision of data-driven knowledge we had witnessed in Chapter 2. Put together, they extend a modern history of 'objectivity', 'technology' and 'data' as regulatory ideals, as composites of collective fantasies. The second half of this chapter thus situates self-surveillance in a broader history of how ideas of objectivity and

---

[88] Deborah Lupton has been developing a similar usage of the term (Lupton 2016). While her full analysis (in monograph form) remains unpublished at time of writing, Lupton too appears to speak of 'sense' both in terms of the biological senses and sense-making as meaning-making.

[89] Here I am using Donald Landes' translation of Merleau-Ponty (2012).

[90] From this perspective, the advent of self-tracking technologies is oriented towards not only an outsourcing of human sense-making to machines, but a corresponding recalibration of human *sens* itself. As Heidegger had already seen, technology's impact on human meaning [*Sinn*] is that of a *displacement* [*Sinnverschiebung*] and consequent reconstitution. The latter is fully achieved when technologies once new, noticeable, *artificial*, become equipment for sensing that human subjects take up habitually and/or tacitly (see Hörl 2015).

technology have shifted over time – and at each stage of that shift, helped organise and legitimate different strategies and virtues for the pursuit of progress and epistemic certainty. In that sense, the present moment is a kind of 'honeymoon objectivity': the buoyance of new promises about old problems, of 'truth', of 'certainty', that reprises older cycles of enthusiasm and pessimism (see Marvin 1988). The discourse of data-sense thus marks a contemporary site for the renewed projection of modernist fantasies, and for the advancing colonisation of everyday life and lived knowledge by the ideals of technological objectivity.

DATA-SENSE

Self-tracking's effectiveness, both concretely deployed and publicly projected, revolved around what we have called machinic sensibility: the ability to extract the kinds of data that are denied to human intuition and experience. Chapter 2 examined how self-tracking's convergence of 'smart' sensors, persistent wireless connectivity and predictive analytics claimed to bypass human error and deliver more accurate, precise, objective self-knowledge. The more users were prevented from 'lying to themselves', the closer to the truth they would get. Yet by the end of Chapter 2, we had identified a contradiction central to this promise: how can an epistemic production line

focused on bypassing the human subject be properly called self-knowledge? Insofar as human subjects' more traditional access to their own data became identified with uncertainty and error, how could such 'raw' data be made intelligible for human subjects? It is this incommensurability between data-driven knowledge and human sensibility that the rhetoric of data-sense seeks to bridge.

We may begin by considering how self-tracking discourse articulated the problems and challenges of a data-saturated society, and thereby asserted the necessity and inevitability of data-sense. If the surveillance state articulated the dangers of 'New Terrorism' precisely to justify the advent of new forms and degrees of surveillance, self-tracking too is defined in terms of the problem it is meant to solve. In this case, that problem was a reprisal of some very familiar tropes that had percolated throughout the Internet age: the idea of data as flood, and as nonsense. First, self-tracking discourse commonly referenced alarms about the sheer proliferation of data, a *flood*. Some practitioners had characterised self-tracking as 'small data', a uniquely individual alternative to the broader emergence of 'big data' (e.g. Cornell 2011). However, the new availability of persistent *streams* of data points – heart rates, galvanic skin responses, kinetic movements, measured multiple

times a second and constantly fed into local databases – soon meant that just like populational data, self-tracking would be beset by the problem of data overload (see Swan 2013; Fawcett 2016). Across state, corporate and self-surveillance, the sheer *comprehensiveness* of this data supplied hopes for genuinely 'representative' datasets as well as anxieties about humans becoming overwhelmed by it. Media commentary on self-tracking – which itself included academics and industry insiders – spoke of 'drowning in data' (Peysakhovich & Stephens-Davidowitz 2015), or having 'too much' data (Brennan 2015), in ways that reprised the narratives of the 'information flood' in the 1990s that had themselves been a response to the public distribution of the World Wide Web. As John Durham Peters notes, sea and seafaring metaphors have always been a staple for cyberspace discourse (2015, p107); they, consistent with the far older history of seas, oceans and ships as metaphors and as media, illustrate the plenitude of data as a rich source of knowledge and control, and yet itself a vastness that defies full capture (p54).

This narrative intersected with another (familiar) problem: data as *nonsense.* How to take a knowledge technique whose central value is in going beyond the human senses, and *translate* it into a human-friendly grid of intelligibility? In the mid-2010s, self-tracking was typically judged as emitting large streams

of data into the world, but still lacking a robust 'action layer' (Swan 2012, p235) that would allow it all to become meaningful to technological laymen. (Goetz 2011) More sceptical actors contended that for all the obsessive and indulgent counting of such 'datasexuals' (see Morozov 2013, Chapter 7; Matyszczyk 2012; Zandbergen 2013), making sense of the data still remains a major obstacle (Singer 2011; Wagstaff 2014; Waldman 2013). In a parallel problem to the enormity and inaccessibility of the Snowden files, QSers and sceptics alike wondered: what kind of knowledge is gained when the human subject gazes mystified at a conflagration of data? (Dancy 2015) It was the 'Big Ass Graph' problem all over again. This concern was situated in a broader set of anxieties about what I have called trace-bodies (Hong 2015); that is, the institutionalised production of identities or profiles on the basis of personal data. Self-tracking came into public awareness even as corporate data-mining was increasingly being criticised as a commercial exploitation of personal traces, an economy which deprived users of knowledge about the contents and production of their own data. At the same time that the Web 2.0 economy in general provoked concerns that "we are [becoming] strangers to our normatively aggregated selves" (Nyong'o 2015), self-tracking was seeking the translational tools it would need to deliver on its promise of empowerment through data and personalised control. Data as flood, as nonsense: both

problems reflected the practical need for a certain mediational structure between machine, data, and human.

It was as a response to such problems that self-tracking discourse posed a 'low-friction', atmospheric vision of sensing machines. In this view, machines and numbers would fade away – much like the wiring for our electricity or the algorithms behind the convenience of social media platforms – and offer a smooth, overarching experience of fast and accurate knowledge. This language itself was cobbled together by translating and popularising contemporary tropes in areas like microbiology and climate science, as well as the more familiar heritage of data metaphors within computing discourse. Gary Wolf (2009b), borrowing from climate scientist Jesse Ausubel of the Rockefeller University, speaks of a 'macroscope'; massively scaled, computer-driven data collection as a way to transcend singular correlations and develop new, data-driven common sense wisdoms about the self.[91]

[91] In his personal blog, Wolf pegs the macroscope as a master metaphor for how he was making sense of the Quantified Self, even as he was involved as a co-founder. Wolf explains that his own book on QS initially began as part of a larger monograph on such 'macroscopes', a notion which he intended to link back to the enthusiasm for measurements and their aggregation into larger pictures of nature as early as the Royal Society (Wolf n.d.). Here, again, Wolf seeks to align contemporary developments in self-tracking with a longer history of scientific inquiry and technical evolution in knowledge production. We shall return to this leveraging of the virtues of scientific objectivity in the next section.

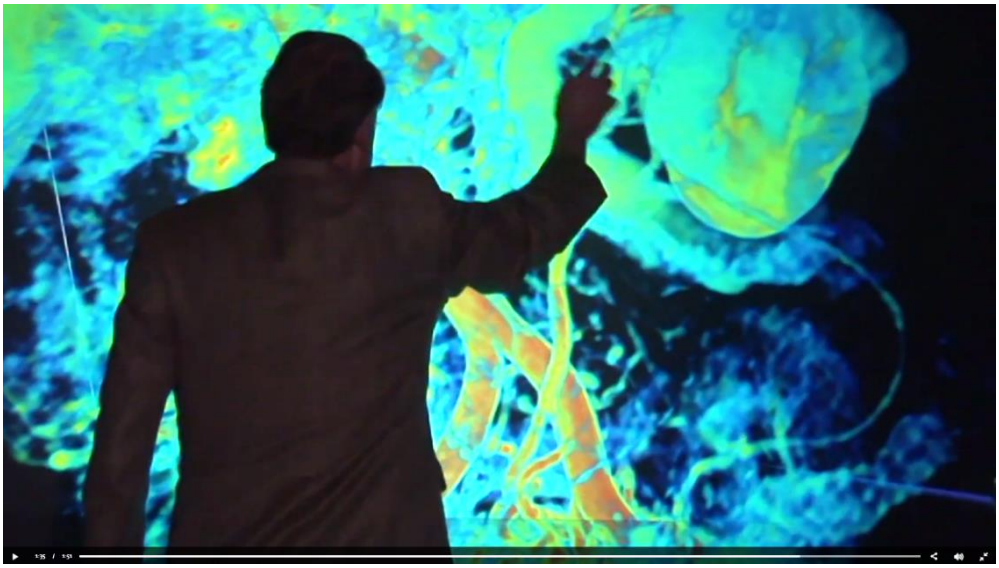


Figure 14. Smarr's microbiome.

One emblematic object in this regard was the human microbiome[92]: the ecosystem of bacteria, fungi, and other organisms that reside in the human body, especially the gut. Typically credited to molecular biologist and Nobel Prize winner Joshua Lederberg in the early 2000s[93], it has since become a popular object of fascination and hope about new breakthroughs in human

[92] While the actual scientific literature now distinguishes between microbiome (the genomes of microbes) and microbiota (the organisms themselves), we shall stick to the 'microbiome' – the term which originally described both, and has since been popularised as an image of the nebula of tiny lifeforms residing in the human gut and elsewhere.

[93] I say typically credited, because Lederberg himself did not coin the term in a discrete and explicit sense, and similar uses of the term was sporadically present since at least the 1980s. (For instance, see a basic genealogy performed by Jonathan Eisen (2015) of University of California, Davis). Nevertheless, Lederberg's own promotion of the term in the early 2000s (e.g. Lederberg 2001; Hooper & Gordon 2001) is now understood as a useful origin point for the subsequent interest in the term and its referent, both inside and outside the scientific community, since then.

health, both inside and outside the scientific community. For self-tracking discourse, the microbiome was a particularly useful depiction of the necessity and potential of such 'macroscopic' technologies for self-knowledge. It is an entire system latent in every human, yet entirely inaccessible to human sensibility. Its composition is unique to every individual, favouring the "n=1" approach of self-trackers over populational norms or the Queteletian *l'homme moyen*. Self-tracking discourse thus latched onto – and amplified – the interest surrounding the microbiome, describing it as an untapped lode of a diverse wealth of new knowledge just waiting to be colonised by tracking tools. This narrative received an appropriately iconic protagonist in Larry Smarr, the physicist who masterminded the foundation of America's Supercomputer Centers Program in the 1980s. Smarr's personal efforts to track his health throughout the 2000s, it was claimed, allowed him to correctly diagnose the onset of Crohn's disease (Ramirez 2013; Cohen 2012). By the early 2010s, he had constructed a chamber at his home institution, Calit2; there, the walls are lined with screens providing a walk-in 360 degree view of his gut and its microbiota (Bowden 2012). Meanwhile, Smarr's experiments had led him to the QS movement, which found in Smarr a pioneering and ambitious example of where self-tracking could lead us to. Cases like Smarr's provide self-tracking discourse with convenient heroic myths. Although Smarr's claim to

concrete, specific achievement in health knowledge required an extraordinary set of personal expertise, institutional backing and other resources, self-tracking discourse could play up his 'success' as a way to bridge the relatively mundane and often failure-prone devices of self-tracking's present with the rhetoric of its transformative future.

And so, Smarr (2012) himself explicitly framed his experiments in terms of a prospective near future where subjects might enjoy a smooth and naturalised access to their own data. Smarr's microbiome chamber, where he can literally move around and reach out towards his data, is a monument to the vision of data-sense: the hope that numbers and machines will soon disappear from the user's experience.

***

We now turn to the specific virtues, ideals, skills, that the discourse of data-sense prescribes for the tracking/tracked subject. These prescriptions ranged from the relatively mundane to the outlandishly futuristic; tracing this range allows us to examine the ways in which the rhetoric of data-sense seeks to flesh out heady posthumanist fantasies in terms of relatively modest products

and experiments, and to bestow the latter in turn with the aura of the former. To begin at the most basic level, we find the idea of data-sense as a certain literacy. In 2012, *Wired* – ever the evangelist for new practices in computing, and the institution whose employees had co-founded QS – hosted *Wired Health Conference: Living By Numbers.* With a focus not only on self-tracking but more professional and institutional cases of health-related tracking, the conference gave QS another opportunity to present its vision to the public. Here, we can locate as a key example the words of Kevin Kelly: the co-founder of the Quantified Self, a prominent opinion leader in self-tracking discourse – and one who, as we have previously noted, had also performed such a role in the utopian visions of the early Internet age.

> We're horribly, I mean, we're just not evolved to deal with numbers. Our brains aren't really good with dealing with numbers, we don't do statistics very well, we're not really a number animal (Kelly *in* Wolf & Kelly 2012; also see Mortensen 2013).

In this case, the narrative remains at a utilitarian and instrumental level: self-tracking is described as requiring new *skills,* akin to the problem of learning the right grammar or typesetting. In this regard, QSers and the self-tracking

industry has long engaged with data visualisation techniques as a way to render those pesky numbers into patterns, juxtapositions, curves: objects which communicate a certain narrative form. Ironically, one example of such visualisation carries the name of Data Sense. Data Sense is a non-profit web tool developed principally by Intel Labs, including Dawn Nafus, a long-time researcher of and participant in the QS community. As a supporting tool, Data Sense measures nothing, but allows users to import, aggregate, visualise and manipulate their tracked data in everything from map overlays to bar graphs. Other projects, mainly artistic, have also drawn on the longer history of wearable computing; examples include a Microsoft Research vest filled with feather-like flaps that move and reshape based on mood metrics (Allen 2014), or Nancy Dougherty (who, we saw earlier, espoused the term 'QS mindset')'s wearable lights that would shift colours as visual representations of her electromyography [EMG] readings (Finley 2013). Such tools aimed to "improve data literacy without making people into statisticians" (*Data Sense* n.d.), providing a supplementary set of communicative channels.

Data-sense often went further, however. If Kevin Kelly spoke above in terms of a literacy or numeracy, he then went on to argue that machinic sensibility can and should be appropriated into subjects' own sensory experience. In this

vision, users would no longer have to struggle with the 'raw' data or even the proliferation of graphs and tables, but become so used to having machinic communications all around them that they would intuitively and habitually reach for input from tracking devices to check whether they are hungry (and what they might be craving), where they are going, and whether they are properly rested.

> But what I think the long term direction of this is, is, we want to use these sensors we're talking about to give us new senses. To equip us with new ways to hear our body […] right now we have to see the data, the charts, the curves, but in the long term where we want to go is, we want to be able to feel, or see, or hear them. (Kelly *in* Wolf & Kelly 2012)

These 'new senses' are thus described as an internalisation of machinic temporalities, rhythms, patterns of communication, into user-subjects' phenomenological equipment.[94] The disjuncture between the rhetoric and its

[94] Sharon and Zandbergen (2016, p6) describes another example of self-trackers' use of the language of 'new senses', this time at a Quantified Self conference in 2014. "At a break-out session, one person told us how he used to take a picture each day at 08.36. For him, this was a way of "developing new senses." He explains, "when I take a picture at 08.36 every day, I have a little better awareness of when it is 08.36." Another tracker added, "when you do it long enough, you don't need the tools anymore." We encountered many more such testimonies to how tracking trained people to be able to "sense" things. In such examples, numerical data are not at all the end-goal of tracking; they are more like an unsophisticated, intermediate stage towards more augmented senses. For some self-trackers, the cultivation of this awareness is more significant than the actual data generated by tracking." Again, there is a folk usage of the language of 'new senses' – one which rarely articulates a systematic theory or mechanism, but instead functions as a shortcut for communicating the transformative potentials of the new technology.

concrete instantiations is striking. For his part, Kelly provided the example of a simple experiment, of unknown provenance: a customised belt that would regularly vibrate in the direction pointing North. Soon enough, he claimed, the wearer had developed an 'unconscious sense' of cardinal directions. Of course, even the humans of the Internet age have not forgotten to read North and South by simply observing the sun. There is little here to prove the actual usefulness of such a 'sense', or any systemic description of 'new senses'; yet such an example was seamlessly juxtaposed, in the discourse, with a far more ambitious vision.

Figure 15. Ling Tan's device.

Others beyond Kevin Kelly joined in juxtaposing the relatively modest commercial products and design experiments to lofty ideals of transformation – whether to advance their corporate appeal, out of genuine enthusiasm, or both. Haptics was a key frontier; if the visual and aural alerts common in personal computers and smartphones were designed to explicitly interrupt the user and enact 'hard' jolts on their attention (Wajcman & Rose 2011), haptic feedback was beginning to experiment with more persistent, backgrounded kinds of responsivity. Just as James Proud's device sought to disappear into the lived environment, gently buzzing wristwatches were promoted as normalising 'low-friction' feedback that human subjects could learn to accommodate in the same way they, say, seamlessly receive information about temperature through their skin (Smith 2015). In another example, one London designer showcased a self-tracking device that would use discomforting or even punishing feedback, including a flare of intense heat (Peters 2013) – pointing towards the extended array of communicative channels between humans and machines that self-tracking devices are beginning to explore. The turn to haptics thus reprises the role played by skeuomorphic design elements throughout the history of personal computing.

Once again, such practices hardly add up to a posthumanist development of 'new senses for new sensors'. The rhetoric of data-sense, ultimately, is about overstepping the reality of existing achievements and attempting to orient public imagination towards the technological future that is apparently just around the corner. This is not to say that self-tracking of the early and mid-2010s did nothing for human mechanisms of self-knowledge. Though relatively one-dimensional in their individual manifestations, self-tracking devices in this period were increasingly cultivating fresh channels for communicating machinic data to human subjects.[95] These channels were being designed not to provoke discrete queries and deliberations, but a habituated and tacit receptivity to the continuous flow of machinic communications. Vision, Merleau-Ponty said, is "the means given me for being absent from myself" (1996, p146). Notwithstanding his complicity in the Western tendency to privilege vision over the other senses (which he acknowledged later in his career), we can apply this thinking to self-tracking's efforts to augment the senses as a whole. To sense one's own body is already for consciousness to direct itself towards something else, an object; self-knowledge, in other words, is to know the 'me' as an object distinct from the conscious 'I'

[95] This process has alternatively been described as 'biopedagogy' (Fotopoulou & O'Riordan 2015).

(Merleau-Ponty 2012). Self-tracking is designed precisely to intercede in this relation. And where concrete deployments often proved as capable of frustrating their users as revolutionising their senses, their mediated public presentation continued to mobilise subjects to consume, experiment, and produce ever more data about themselves.

This imagined reconfiguration of the subjects' sensory equipment, and the emergence of a pervasive communicative circuit between selves and their sensors, reached its rhetorical peak in claims of a broader, posthuman shift. Kevin Kelly elsewhere christened it *exoself*: an 'extended connected self' that constantly discharges data while receiving all kinds of machinic communications, both consciously and non-consciously (see Swan 2013, p95). Such language extends the long narrative of technological transcendence that had characterised utopian (and some dystopian) rhetoric about personal computing and the Internet in previous decades – and, indeed, the broad and powerful influence of cybernetics throughout the 20th century that defined the body and the selves as information systems (see Hayles 1999; Lupton 2014). One particularly relevant branch of that cybernetic imaginary had been the countercultural influence on personal computing and the Internet as a route to a technologically expanded consciousness – a vision that Kevin Kelly

himself had actively brokered in the 1980s and 90s (Turner 2006). It was in extension of this context that self-tracking enthusiasts across news media, internet technology industries and the Quantified Self movement spoke of exoselves and new senses. Such discourse promised not a future where users are turned into hyper-rational machines, but rather a more 'authentic' relationship to one's own humanity.[96] Thus we find 'innovation design consultants' claiming that self-tracking "technology will offer a level of self-awareness that could make us more human than ever" (Brennan 2015) – or the founder of a self-tracking headset company proclaiming the advent of a 'humanising technology' (Garten 2011).

***

The rhetoric of data-sense, then, ran the full gamut: from more modest and practical descriptions of new skills and literacies, to futurist fantasies of the impending 'exoself'. Such narratives focused on the transformations apparently affecting the human senses and the phenomenological self. At the same time, self-tracking discourse also featured a set of ideals and

[96] For a discussion of such rhetoric of authenticity through self-tracking vis-à-vis health and well-being, see Sharon (2016).

expectations about how the practice could develop into a social/commercial structure. In other words, the perceived benefits of data-sense were not limited to individual satisfaction. Parallel to smart machines' increasing tendency to share data and align their interventions across each other, a shared set of literacies and sensory configurations were already allowing self-tracking communities like QS to communicate and coordinate. As Theodore Porter (1995) argues in his history of quantification, the intersection of quantification as method and objectivity as ideal often had the political consequence of facilitating the public sharing of information and consensus-building – even as those actors remain strangers without other kinds of shared context. Although the Quantified Self community refused any dogmatic or standardised implementation of quantitative metrics, and encouraged highly personal forms of hacking / experimentation, familiar mainstays of the modern day scientific method were often recruited by QSers to discuss each other's experiments. Discussions of how one QSer's system for measuring mood could be replicated, or whether an experiment in the correlation between protein diets and bowel movements featured a control condition, worked to organise these eclectic practices into a broader program of inquiry and collective knowledge. Gary Wolf thus describes the community as a place where the roles of consumer, user, developer, expert

become entangled, allowing every participant to contribute to this process from

> a position of equality with the experts who design that stuff […] And nobody stands higher than them on that passage of discovery […] So that, for me, is sort of the magic. Where the experts interact more personally, and the people interact more expertly. That underlies my sense of what's different about Quantified Self from just, some kind of lifestyle trend where people pick a gadget, and put it on.
>
> So it's kind of an idea about how to make knowledge together, or how to reason together, that I think is, it's interesting to talk about now because the tools exist to make it easier for us to reason together this way, and I think it's this style of reasoning that I [...] is the Quantified Self (Wolf 2015, personal communication).

In other words, QS functions as a kind of Fleckian (1979) thought collective: a social space where the repeated exchange of ideas produces emergent norms regarding what counts as sufficiently reliable data, rigorous test, and valid conclusion; for instance, one finds a widespread scepticism of 'one size fits all' solutions, from over-the-counter pills to the body mass index (not to mention attempts to generalise findings of any singular self-tracking experiment). Although QS' founders and voluntary meetup organisers tended to shy away from explicitly defining 'best practices' in self-tracking, seeking instead to promote an inclusive, decentralised atmosphere, the QS meetups, websites

and conferences served as a *social* space for curating attitudes towards self-tracking.

The Quantified Self, of course, only accounted for a specific subset of the growing self-tracking market; hence I described the former as a *connoisseur* community, and the latter as a population of *laypeople,* in the Introduction. Just as virtual communities of the 1990s represented a larger and increasingly commercialised uptake of earlier, experimental communities like the Homebrew Computer Club and the WELL, the tinkering enthusiasts that made up the Quantified Self communities is increasingly being dwarfed in population by what is sometimes labelled the Quantified Us: a vast network of publicly shared personal data that allows intersubjective and populational patterns to be drawn (e.g. Jordan & Pfarr 2014; Cha 2015). And therein is the irony. As we noted in Chapter 2, self-tracking discourse in the late 2000s and early 2010s tended to position the practice as the personal, empowering 'n=1' alternative to state and corporate surveillance; that is, as a DIY solution whereby savvy users could take control of the personal data that new technologies were already extracting and exploiting for profit. When Gary Wolf (2010a) advised the globally distributed QS meetups on best practices, one of them was to 'avoid business pitches'; the many 'show and tells' I

observed, both in person and via video recordings, similarly emphasised personal narratives of discovery and experimentation over sleek product promotions or marketing rhetoric about monetisation or target audiences (even when the 'personal' show and tell was by an entrepreneur and about his/her new tracking product!). Yet as self-tracking devices and practices began to reach the wider, lay population through the success of devices like Fitbit, the massive production of new kinds of personal data by these eager consumers began to open up new horizons for big data, populational norms and corporate profiteering. Although the latter has typically been (noticeably) absent from the public presentation of self-tracking, we can witness an example of the industry logic from a public relations trade magazine's coverage on the matter. In the below excerpt, the said coverage quotes a London-based digital PR professional:

> The opportunity for brands now is to tap into the data the new wave of connected consumers are happy to broadcast so that they can learn more and engage […] What this all means for the PR person is a more tech-savvy approach to understanding consumer behaviour and figuring out how to capture and capitalise on a new kind of attention (Benvie *in* Moore 2013).

If on the object side there is an effort to knit the many tracking systems into a more comprehensive ecosystem, the subjects of self-tracking are also being

enjoined to develop an ethic of voluntary sharing for the 'greater good'. In the context of health tracking, one *Wired* article proclaimed that sharing your intimate details "may be the best decision of your life":

> But if we truly want to enable the breakthroughs and behaviour changes that will transform our health, we must be willing to share our most personal asset: the data about our lifestyle, state of health, and disease (Seidenberg 2014).
>
> Imagine a future where self-tracking harnesses a whole population's data to identify patterns and make meaningful recommendations. Imagine a future where we can see into the data of people just like us, to help us live better, and where we willingly give up a bit of privacy in exchange for vast benefits (Jordan & Pfarr 2014).

Such discourse presents the Quantified Us is presented as an unproblematic upgrade – a smooth 'scaling' that will bring the benefits of self-tracking technologies to more people, and thereby amplify their positive effects. Yet this injunction to share your data for your own good exhibits striking similarities to how corporate data-mining mobilised Web 2.0 users for their own exploitation in the personal data economy. José van Dijck (2013) calls it the culture of connectivity: how social media platforms like Facebook achieved widespread adoption by offering human *connectedness* without a monetary price, and subsequently began extracting and selling this very network of (inter)personal *connectivity* and its vast troves of voluntarily

submitted data. This bargain of apparently 'free' sociability and convenience for our 'free' production of data for others' profit is a defining feature of digital economies in the early twenty-first century. For instance, finds formally analogous structures in the 'free labour' (Terranova 2000) that produces cultural and informational goods in the Web 2.0 economy, from Wikipedia content to maintaining virtual communities. It is no coincidence, therefore, that self-tracking's vision of empowerment through data production dovetails seamlessly with the industry's hopes of tracking individuals as data producers, whose output can then be harvested and commercialised. Neither is it accidental that issues of data privacy, so central to the debates around state surveillance, have tended to remain on the periphery of self-tracking discourse. This is not to suggest a conspiratorial explanation, where QS founders or self-tracking entrepreneurs harbour secret plans to steal users' data. The correlational epistemology underlying big data's favoured techniques – like machine learning and Bayesian inferences – are designed to benefit from as much data as possible. Just as state surveillance systems' 'collect 'em all' strategies were born out of an epistemic data hunger, the developers of self-tracking solutions often end up advocating that sharing is 'worth' the cost in privacy by virtue of their own methodologies.

Even leaving aside the commercial aspect, it would still be naïve to consider the rhetoric of data-sense as a manual in self-empowerment and control. Data-sense seeks to instill in self-tracking's subjects a strong orientation towards efficiency and optimisation in the most mundane and private aspects of their lived experience; hence, the very principles that govern technological development are transposed onto a set of ethical 'best practices' for the subject. Taking the example of Bob Troia, an entrepreneur and QSer who had tracked everything from diet to glucose levels and physical location, Deborah Lupton (2014) suggests that self-tracking instils a more or less neoliberal ethic of ceaseless self-management, through which subjects sign up onto an indefinite cycle of quantified progress; in Troia's own words, "an optimal human being in every aspect of [one's] life" (Troia *in* Lupton 2014). Indeed, this is a narrative for which there is no shortage of spokespersons amongst self-trackers themselves. Elsewhere, Troia claims:

> You track all those issues, and you're like, 'Wow!' I thought I felt great, and then you realise that you've sort of been going through life for a while with the parking brake on,' Troia said. 'And when you start fixing all of those areas, you're like, 'Wow! I didn't realise.' It wasn't that I felt bad, I just didn't realize I could, I *should* be feeling better (Troia *in CBS News* 2014).

It is not difficult to find even more bullish statements that more or less equate self-tracking with the mythical elixir of life:

> Indeed, why not give yourself an 'upgrade', says Dave Asprey, a 'bio-hacker' who takes self-quantification to the extreme of self-experimentation. He claims to have shaved 20 years off his biochemistry and increased his IQ by as much as 40 points through 'smart pills', diet and biology-enhancing gadgets (Dembosky 2011).

To be sure, rhetoric like Asprey's would count as outlandish, if not downright dishonest, for many self-trackers. Yet it is only an extreme rendition of the same kinds of objectives that individuals like Troia also orient themselves by.

Self-tracking discourse's exhortations towards data sharing and relentless self-improvement attracted a host of criticisms – just as its promise of automated and intimate self-knowledge prompted the backlashes described in Chapter 2. The very aspects of self-tracking that the rhetoric of data-sense described as virtues became targets of criticism and sometimes ridicule. First, the language of optimisation and improvement was criticised in those very terms, and decried as a dehumanising obsession:

> It's often easier to understand what to do with data than to evaluate how you feel, and devices that can quantify your walking or blood pressure or vaginal strength let you take advantage of that […] But the

> pitfall of data devices – and the external sharing of information that they encourage or require – is that they hijack your reward pathways. Instead of walking because it makes you feel good, or because it gets you out in the air or (my personal favourite reason) because sometimes there is bonkers stuff to see in between point A and point B, you walk in order to improve your stats (Zimmerman 2014).

Similarly, self-tracking's promise of personalised knowledge and exhaustive attention to the well-being of the individual self was targeted with accusations of *narcissism* – a trope so commonly voiced in media representations of self-tracking, that Gary Wolf (e.g. 2010b) acknowledged it in his own pieces defending and promoting the Quantified Self. (In a self-deprecating nod to such criticism, Wolf (2009a) in fact ran psychological assessment surveys on a sample of QSers – to quantify the narcissism of self-trackers!) Although most accusations of narcissism were directed literally at the psychological profile of individuals willing to devote large chunks of their daily life to such tracking activities, it also reflects a key difference between self-tracking as an ethic and the utopian visions of its predecessors in the countercultural influence upon personal computing. If virtual communities of the early 1990s were defined by a technological optimism about building new forms of social organisation and spreading information to the far corners of the earth, the talk of 'new senses' or the vision of the Quantified Us is squarely focused on each individual's betterment of themselves. The

transcendent revolution promised by the rhetoric of data-sense is thus literally narcissistic – and in ways that extend the Web 2.0 era's economic model of leveraging subjects as voluntary producers of 'free' personal data that can be used to sell new products back to them.

We should be careful, however, not to cleave the landscape into a neat binary division of oblivious trackers and their critics. We find a certain tension between the mass market, populational principles emblematised by the idea of the Quantified Us, and the more eclectic and experimental values often expressed by QSers. At the 2015 Quantified Self Conference, Dawn Nafus – who had built the Data Sense tool with Intel Labs – and Anne Wright, a QS community ('meetup') organiser in Pittsburgh, spoke in no uncertain terms about the 'tyranny of the norm'. Gary Wolf, who was chairing the session, commented that he had recently seen a tracking service advertise, 'compare yourself to the global norm' – a vision which he later told me is "severely perilous":

> I quoted that advertisement, compare yourself to the global norm, and I questioned it a little bit […] The reason I questioned it a little bit isn't because I think it's a little bit questionable [laughs] um, but because I think it's severely perilous […] Because I think that when you think about being in a world where you're constantly comparing yourself to global norms, like, comparing yourself, right there is a problem for

> people […] When you hear this, ask yourself, is that what you want? Or is that what you want to make? Tools that take people and compare them to global norms? (Wolf 2015, personal communication)

The various actors across QS and self-tracking thus overlap messily across different kinds of values, benefits, principles of practice and commercial interests. These struggles, whether amongst self-tracking practitioners themselves or with its critics, show that visions of data-sense, and the publicisation of self-tracking in general, have strong moral and ethical stakes for their subjects.

***

All in all, the rhetoric of data-sense presents a broad array of skills, sensory interfaces, moral virtues, and forms of communal organisation – all of which demarcate the role and identity of the ideal self-tracking subject.

Early twenty-first century citizens were told that to track, and to get 'the best' out of your tracking, they had to develop a new subjective position and ethic – just as previous generations had done with the advent of the Internet and other technologies of knowledge production. Such a narrative enlisted a highly celebratory history of computing technologies in the 20th century; there

is no room for the military-industrial complex, or worries about relentless commercialisation of what was once called 'virtual communities', in this storyboard. In this way, self-tracking was presented to the public as a next step on the march of technological progress – a new epistemic reality that subjects simply had to get used to by accumulating new senses:

> One of the mantras around Quantified Self is that obsessive self-trackers may look outrageously geeky now, but they will soon be the new normal […] we all will be living in an ocean of data in the near future, whether we are self-tracking or not, and learning how to read, manage, retrieve, understand, digest, parse, and selectively ignore this flood of data will be an essential skill – for individuals and for organizations. Self-trackers are there first (Kelly 2011; also see Lupton 2013).

The *new normal*, of course, is exactly the label that contemporaries of September 11 attached to "signify a world destabilised by terrorism, economic fluctuations, and contagion prevention" (Bratich 2006, p493). Like 'new media', the new normal was a presentist description of what early twenty-first century commentators experienced as radically disruptive. And both New Terrorism that is the NSA's bogeyman, and Kelly's 'new normal' of data plenitude, argued that a new set of epistemic practices were simply *necessary* to keep up with the objective reality of our worldly environment. The parallels across the two cases here run deep. The watchers of the state

projected a post-September 11 geopolitical reality that was argued to be unprecedented in dangerousness and unpredictability; such states of affairs, they could then say, *necessitated* their decisions towards powerful and indiscriminate electronic surveillance. In self-tracking's case, such necessary 'reality' took the form of 'obligatory technologies' (Chandler 2012); the likes of Kevin Kelly (Wolf & Kelly 2012) insisted that "something is happening with this new ability" – that is, the new availability of cloud-connected smart sensors – and that subjects must keep up with it to thrive in the technological future. In the case of state surveillance, uncertainty was the rapidly growing spectre that threatened national security, and thereby required ever more data-hungry forms of surveillance; in the case of self-tracking, uncertainty is that old enemy of self-knowledge and self-realisation that might finally be vanquished through the newest sensors. And for that, the vanguards of self-tracking argued, the users too needed to upgrade.

Upgrade. In keeping with the computational metaphors, the human subject is seen to provide an underlying set of functions and frameworks; memory, vision, cognition, reason… and these capabilities, it is argued, can be newly programmed and augmented in order to stay compatible with increasingly sophisticated technological prostheses. Data-sense is thus what Peter Freund

calls – mixing metaphors across Elias and Bourdieu – a *technological habitus*: the social tempering of the body that allows individuals to internalise the virtues, senses and knowhow necessary to prosper in that technological society (Freund 2004). It is through this process that subjects achieve the kind of efficacy or competency that 'counts' in the new regime of knowledge, whether it be the savvy social media user that extracts reputational and monetary rewards through the network, or the self-tracking connoisseur who can skilfully comprehend and manipulate the new wealth of personal data. And just as state surveillance seeks unprecedented transparency on the part of the population in order to read its criminal intent, self-tracking's ability to make one's own body more transparent to oneself produces its own grid of legibility for a broader set of actors: from employers interested in optimising the biopower of its human resources, to insurance companies which are already offering discounts in exchange for access to ratepayers' Fitbit data (Mearian 2015), and more besides. The project of knowing more about and optimising the self enrols many different commercial, business and government interests.

In short, data-sense describes the widespread discourse that exhorted the necessity of a new kind of user-subject. Analogous to the creation of the user

(Hu 2015), the netizen, and other subject figures in recent decades, this interpellation was a sustained effort at codifying and organising the masses to adapt their epistemic processes, their ways of seeing, in ways that would facilitate the normalisation of self-tracking technology as epistemic schema and marketing foothold. In tandem with the design, function and rhetorical presentation of the technological objects in Chapter 2, data-sense thus constituted a comprehensive vision of a posthumanist subject – one that would eradicate, or at least minimise, long-standing uncertainties in self-knowledge. Where electricity's contemporaries dreamed of ghostly communication and the annihilation of space and time (Marvin 1988, Peters 1999), and the Internet's contemporaries dreamed the end of state divisions or physical distance (Flichy 2007), data-sense articulates the presentist imaginaries that give buoyance to an emerging technology. And just like those earlier cases, many of self-tracking's most ambitious visions are unlikely to be realised in such purity. Their significance is not in their prophetic value, but their current role in interpreting, circulating and framing the technological deployment. Data-sense thus helps organise not only what counts as knowledge and the uncertain, but how subjects themselves should become adequate receivers, users, circulators of that epistemic regime.

HONEYMOON OBJECTIVITY

Data-sense as a programme for self-tracking subjects derived its veridical authority and epistemic structure by relying on an existing set of metaphors and narratives, of prescriptive norms and ontological presumptions. In doing so, they extend a history of ideas that stretches back not only to the language of the cloud, the user, cyberspace and virtual communities (e.g. Hu 2015, Turner 2006, Chun 2006, Flichy 2007) but to the very birth of the terms 'technology' and 'objectivity' in their modern form. Objectivity, technology, and data, especially 'raw' data: these concepts serve as bedrocks for self-tracking's claims towards 'humanising technology' or better self-knowledge. This section thus situates data-sense in the history of those very concepts and the epistemic visions they had previously endorsed. Data-sense is 'new' in its specific mélange of posthumanist ideals, machinic sensibility and data-driven environments, but the kind of role it plays in the social life of new media technologies reprises previous historical shifts under the name of objective truth and technological progress. In this context, we might characterise the epistemic promises of data-driven surveillance as a kind of 'honeymoon objectivity': a fascination with nascent technologies as the skeleton key to truth that exhibits a certain cultural amnesia, reinforcing a binary narrative

between an idyllic 'pre-technical' subject and an equally fantastically posthumanist one.

Objectivity, as extensively chronicled by Lorraine Daston and Peter Galison (2007), had older renditions like the scholastic *obiectivus*/*obiective*, but generally enjoyed definitions starkly different from the modern. Even in Kant, objective validity meant general 'forms of sensibility' that prepare experience, while it was the 'subjective' that referred to specific and concretely empirical sensations. They argue that it is only during the 19th century that develops the now familiar juxtaposition: a neutral, 'aperspectival' objectivity as the privileged instrument towards truth and scientific inquiry, and biased, unreliable subjectivity as its nemesis (also see Daston 1992). Most relevantly for our analysis, these movements produce by the late 19th century what Daston and Galison call 'mechanical objectivity': a regulative ideal which called for the excision of the human observer from the process of data visualisation (in this context, scientific atlases). In this case, it was the technological development of photography that spurred new linkages between automation and objectivity, producing the ideal where "machines [would be] paragons of certain human virtues" (Daston & Galison 2007, p123), and the most truthful representations of natural data would be the least

subjective, 'entirely artless' (p133). The rhetoric of data-sense thus leveraged a far older historical value of objectivity, with the cultural capital it had accumulated through traditions of scientific inquiry.

Mechanical objectivity does not, of course, encompass the many different renditions of the ideals of objectivity in Western societies since the 19th century. It does exemplify how much contemporary uses of the concept – including within self-tracking discourse – owes to these developments in scientific inquiry. The rhetoric of data-sense is thus literally parasitic: its combination of tinkering ethic, technological enthusiasm and consumer market ambitions latches onto the lexicon, epistemic assumptions, and social authority of what had originally been part of the effort to define 'good science' and the truth of nature. Self-surveillance – and, indeed, in many ways, state and corporate surveillance – thus expounds the virtues of automation, quantification, machinic sensibility, 'bigger' data, all in the name of achieving greater objectivity, understood here as an unchanging and factual knowledge of reality purged of human bias. If Emotion Sense quantifies 'mood' onto a scatter plot graph, an intrepid individual embarks on a quest to inventory every single possession and index them by market

price[97], and even pelvic floor muscles are subject to real-time tracking and haptic feedback (kGoal), it is repeatedly stated that all this is for the sake of a more objective – sometimes 'scientific', 'accurate' – knowledge. We thus find, amongst self-tracking practitioners and enthusiasts, the argument that self-tracking can provide new degrees of objectivity formerly denied by inadequate technologies. Consider the following examples, the first by a technology reporter, the second by Joseph Kvedar, the Director of the Centre for Connected Health at Harvard Medical School (also see Swan 2013, p92; Crawford et al. 2015, p492)[98]:

> The way it is measured right now requires episodic periodic visits to a neurologist, who puts patients through fairly subjective and coarse clinical tests—there are many 1-2-3-4 scales. What we need to advance is research that is a much more consistent and objective measure of the disease (Ungerleider 2014).
>
> On weekends when I had to do yard work instead of cycle, I resented it as a waste of time. This all changed about a year ago when I was looking at the stats from my Bodymedia armband. I discovered that I

[97] Such was the self-tracking project of Matt Russell, which was shared with a New York QS meetup in 2015. He had compiled a database of every type of possession, from perishable groceries to furniture and sentimental keepsakes, analysing them primarily as a way to optimise and 'get in front of' his consumption rhythm.

[98] Sometimes, researchers and professionals in health and information technologies also helped circulate a confident rhetoric of progress towards objectivity. For instance, consider a 2014 article published by the Institute of Electrical and Electronics Engineers [IEEE], one of the largest such associations globally, and authored by two computer science researchers at University of California, Irvine: "Historically, we have gone through the following phases of understanding the self: anecdotal, subjective diary, and quantified self. Lately, there has been a lot of talk about the quantified self. Soon we will enter the most scientific stage: the objective self." (Jain & Jalali 2014)

> burn about 1.5X the amount of calories per hour of yard work as I do cycling […] The result of that insight is that I welcome my days of yard work now […] This is a perfect example of how objective, quantified information can lead to insights that prompt behavior change. We are in the midst of a real movement around the collection of data and the use of that data to gain insight about health and affect behavior change… (Kvedar 2011)

Such language leans on objectivity as a venerable, reliable quality, one whose virtues and authority is hardly in question. Yet as we have mentioned above, to invoke objectivity is to leverage a regulative ideal that is itself a composite of different virtues and epistemological claims – and a composite whose organisation has itself changed constantly over its history. Accordingly, the rhetoric of data-sense also performed a degree of conceptual localisation. For his part, Gary Wolf stresses that objectivity should not be understood as a rigid, dogmatic commitment to numbers, but an intelligent leveraging of machinic virtues like regularity, precision, reliability. In this articulation, objectivity is a way to formally standardise what is also, paradoxically enough, a personal and eclectic practice. In our interview, asked about QSers' discussions about 'subjective measurements', Wolf offered an *ad hoc* schema of objectivity vis-à-vis tracking practice:

> One is objective means explicit. And you could say formal, in that sense. Numerical. So if you think of it in terms of representation, you could classify types of representation from formal to informal […] and

> on the formal side you have, you know, logic, numerals, and things like that, and somewhere in the middle you have words, and maybe all the way on the right hand side, if we're doing it that way, you have music, or, you know, colour fields painted in […]
>
> Another is social versus individual, in which individual perception would be considered subjective, and social – an idea, a perception, an observation that entailed agreement of more people, whether that be expert observers or everybody, would be objective. So there's an interesting history of that word, you know, and the way in which the formality of expressions and the sociality – the formality of expressions has a sociality, a credibility – became so tightly tangled together under the term objectivity. I think that they probably have to come apart to understand the Quantified Self, and the objectivity of the Quantified Self really refers to the way it's actually used. It refers to formality of expression. And not so much to a kind of social validity (Wolf 2015, personal communication).

A 'subjective' measure like self-reported mood scores may never attain 'objectivity' as an ontological quality, objectivity as a faithfulness to aperspectival reality; but, Wolf argues, "what you can do is work with them and think with them" (ibid.) precisely insofar as they are 'formal'. Such an articulation seeks to square QS' commitment to personalised control over data and self-knowledge, with the legitimation of that knowledge through its demonstration of a formal objectivity. Such folk theorisation hardly adds up to a comprehensive philosophy. The attempt at making sense of objectivity vis-à-vis self-tracking, however, reflects the continuing movements at bridging scientific objectivity and the tinkering ethic, and a bid to establish the wider epistemic legitimacy of the practice. One part of this effort has been

the gradual weaning of the self-nominated 'Quantified' prefix; an effort to preserve the virtues of formal, standardised, machinic objectivity beyond the stereotypes of inhumanly hyper-rational number geeks. Indeed, Gary Wolf's 'state of the movement' piece in the *New York Times* (2010b) was keen to differentiate self-trackers from the figures like Charles Dickens' Mr. Gradgrind. Where Gradgrind was an insufferably 'obstinate' stiff who insisted his pupils chant 'Fact, fact, fact!', Wolf insisted, "it is normal to seek data". In this vision, self-tracking pursues objectivity not as a dry and scholarly insistence on precise factuality, but a practical virtue that seeks the eradication of biases, errors, and other forms of epistemic uncertainty when it comes to self-knowledge. If state surveillance relied on its simulationist heuristics for 'actionable' knowledge, Wolf's QS seeks to produce everyday reality in forms that can be compared, tabulated, manipulated, optimised – that is, "amenable to computing" (Wolf 2015, personal communication).

Wolf's description matches much of what I have witnessed in my own participation at meetups and conferences. Still, no single definition applies dogmatically across the many different invocations of objectivity in the self-tracking context. It is not even necessary for every practitioner to subscribe to the same definition in order to participate in the vision. Terms like

'objectivity' encompass a certain range of uses and interpretations, and indeed, the great advantage of this 'strategic ambiguity' is to provide a linguistic space where many variant positions can congregate and communicate (Eisenberg 1984). Within this 'range', the common language of objectivity, and its accumulated historical *gravitas,* provides a space for some flexibility, some hybridisation, in navigating the tensions between the grand narrative and local epistemic processes.

This transposition of the virtues and legitimacy of objectivity also extended to the figure of the ideal knowing subject. If objectivity in many contexts developed a suspicion of subjective claims, and often sought to inoculate its procedures from human tampering, this also meant that ideals of objectivity had to strictly regulate the kinds of subjective virtues and practices that are necessary to secure the former. The rhetoric of data-sense thus extends and leverages not only posthuman fantasies of the digital age, but the idea that objective knowledge requires corresponding discipline in its subjects. Daston and Galison describe, in terms of mechanical objectivity, an injunction to 'self-surveillance' on the part of scientists; a deliberate curbing of the temptation to subjective bias and projection. The ideal subject of this epistemic regime would transcribe, illustrate, and interpret exactly what the mechanisms of

photography and later microscopy would yield; a patient and diligent work of suppressing the subjective that they compare to Schopenhauer's 'will to willessness' (2007, p174-6, 203). The subjective virtues of objective epistemology was not limited to a disappearing act. Theodore Porter (2014) points out that the human champions of mechanical objectivity were also expected to exhibit a set of moral traits – traits that ironically included the ability to confidently *imagine* a utopian future for such science. And at a practical level, where the work of machines is inevitably handled, interpreted, regulated by human hands and eyes, the ideals of objectivity translated – at least in the increasingly institutionalised and professionalised halls of 'normal' science[99] – into the valorisation of qualities like reliable and dependable personalities (Daston 1992, Shapin 2008). To articulate the virtues

[99] This historical shift has elsewhere been described as the passage from science as the early modern pursuit by individual, often polymath amateurs to professional specialists as part of larger and more rigorously regulated institutions. For instance, the early members of the Royal Society were associated with and contemporaneous with the English adoption of the term *virtuoso* / *virtuosi* – which designated amateur dilettantes whose inquiries into nature were less regulated, highly personal, and driven by the *pleasure* of knowledge (e.g. Houghton Jr. 1942, p61; Musson & Robinson 1969, p20; Eamon 1994). This is in stark contrast to what Steven Shapin (2008) calls the 'industrial scientist' of Cold War America; a system of funding, organisation, and often state sponsorship that would emphasise the scientist as a 'honest, sober, dependable' professional employee of the larger system. And of course, the very founding of the Royal Society, including its Baconian influence, was part of a concerted effort towards a more systematic and methodical production of scientific knowledge (Hunter 1989; Rossi 1970, x-xi; Zilsel 2000, p5). To be sure, such a narrative applies more or less to what Kuhn (1962) called 'normal science', which itself continued to be formed and reshaped through transgressive 'revolutions'. Hence, historically, the rise of objectivity and professionalised science over the 19th and 20th centuries also saw a parallel 'track' where figures of heroic genius, with their exceptional subjective touch on the passage of science, could be interrogated (e.g. MacLeod 2007).

of objective knowledge is to specify a subjective ethic that cultivates sufficiently disciplined practitioners. It is in this context that the rhetoric of data-sense leveraged self-tracking's embrace of objectivity towards its own ideals of data literacy, exoselves, and the 'new normal'.

***

If data-sense piggybacks objectivity's authority as an epistemic virtue to instruct a set of subjective ethics, this relation is itself brokered through 'technology' as a complex of different visions and ideals. This again reprises a longer historical pattern. In the case of mechanical objectivity in the 19th century, Daston and Galison (2007) specifically linked its rise in the practice of scientific atlases with the development of new photographic technologies. More importantly, technology as an idea itself brings to the table a host of narratives about the virtues of such epistemic projects. The term technology in its modern sense was only introduced in the mid-19th century, when earlier designations of the practical arts and crafts was disrupted by the breakthrough of industrial machinery. Just as many contemporaries of data-driven surveillance and 'big data' today speak of the coming ubiquity of new technologies, commentators in this period perceived a proliferation of

machines that reflected an unprecedented rate of invention and progress – a perception which, given the extraordinary expansion of material wealth and mechanical infrastructure Europe and America achieved during the Industrial Revolution, was hardly groundless (Landes 1969). If the 'mechanical arts' referred to specific practices of tinkering and craftsmanship, the accession of 'technology' as a term marked a new belief in, well, *technology* as a broad, hyperobjective system – the iconic object being the railroad networks (Marx 1994, 2010). These imaginations of technology as a universal system and an engine for progress would become steadily normalised over the ensuing decades. The mid-20th century critical rhetoric of 'autonomous technology' (Winner 1977), 'technics' (Mumford 1963) and the technological society (Ellul 1964) serves as a way to recognise the kind of authority the term had accrued by cold war America.[100] In other words, it was through specific waves of sociotechnical transformation – emblematised by the railway, electrical power, the industrial factory, the atom bomb, and now the Internet / the Internet of Things – that technology aggregated its modern vision of progress, innovation, and optimisation. Technology, in comparable ways to objectivity, drew together a set of normative assumptions about the virtuous (and/or

[100] It has been claimed that technological advancement was specifically adopted as a key marker of progress for America as a nation, succeeding the vision of Manifest Destiny as settlers – and railroads – completed the journey West by the late 19th century (see Smith 1994; Sarewitz 1996).

dangerous) power of machines and their role in the passage of history. Self-tracking's futuristic vision of automated self-knowledge rode the coattails of this long historical wave, a long maturing set of fantasies – and leveraged those tropes to full effect.

Self-tracking, as a promise of technological advancement in objective truth, exemplifies the mutual exchange of legitimacy and norms across objectivity and technology. Here, we must understand the function of 'technology' as a concept, as an image, as distinct from the deployment of actual and specific technologies. One consequence of the increasing complexity in technological systems was that "the public increasingly had to rely on *images"* – that is, narratives and emblems for popular consumption and imagination – "of technology for its understanding of both technology and progress" (Smith 1994, p40). It is at this level that data-sense profits from the 'image' of technology as a 'neutral' solution or optimiser that can be applied to every problem (see Edgerton 2010; Kline 2001). Once again, corporate data-mining plays the vanguard and engine to self-tracking. Between mid-2000s and the mid-2010s, social media platforms built up a powerful position of authority as institutions for the circulation of both human sociability and commercial sales of personal data based on that sociability. They did so precisely through a

politics of neutrality – a discursive strategy that relied on the common understanding of technology as a neutral and impartial solution to route massive social and commercial influence unto a select few corporations (e.g. Gillespie 2010). Here, it was the claims of *empowerment* and popular sovereignty that became the unwitting dummy for the surveillance and exploitation of personal data (e.g. Van Dijck 2013). Consistent with these earlier developments, self-tracking's vision of personal control has tended to encourage a vision of what Evgeny Morozov (2013) calls 'solutionism': that any and every problem can benefit from technological optimisation, that technology can insert itself as a neutral booster to almost any kind of knowledge problem.

> Anything that is trackable is being tracked. Heart rate, also heart rate variability […] EMG off the muscles, EEG, ECG. You know. Steps, of course, with digital pedometers. Activity level in general. Sleep. Phases of sleep. Location. Social relationships. Mood. Really, almost anything people care about is being turned into something that can be interrogated, using numbers in the broadest sense (Wolf *in* Wolf & Kelly 2012).

Combined, the vision of data-driven surveillance as a neutral optimiser, a next step in society's ineluctable progress towards objective truth, was

christened through its own set of metaphors and images.[101] In the mid-20th century, the Whole Earth Catalog adopted the first image of the whole earth from space as an emblem for its vision of technological transcendence (Turner 2006), even as Marshall McLuhan spoke of the 'global village' (1962, 1964). By the 1990s, the popularisation of the Internet occasioned metaphors of cyberspace, virtual communities (Rheingold 2000), and the 'information superhighway' (see Hu 2015, pxxiv). Self-tracking itself tapped into a set of metaphors governing the broader fascination with (big) data and its wireless circulation. This included the 'cloud' – a vision of smooth, immaterial technology, free of political and physical obstacles, and also the vision of a certain epistemic proliferation, all of which forms a "topography or architecture of our own desire" (ibid., pxvii).[102] Personal data itself received new and often grandiose descriptions: "data is the new oil" was the buzzword in the mid-2010s, expressing again the universalist idea that every phenomenon in our society was an opportunity for 'datafication' to derive new commercial value (e.g. Watson 2015). Most relevantly for self-tracking's specific vision, personal data has been compared to an identity, a body, a

[101] The organising role played by metaphors was comprehensively covered in (Lakoff & Johnson 1980).

[102] If the technological achievements of earlier eras produced imposing physical monuments to their transformative ambitions, producing a collective awe and recognition that has been called 'the technological sublime' (Nye 1994), it is such immaterial and hyperobjective symbols that fulfil a similar role in the new media society.

double, a dopplegänger, a profile, a DNA (Cheney-Lippold 2011; Raley 2013; Bauman & Lyon 2013; Haggerty & Ericson 2000; Watson 2014). In this language, data is an ubiquitous, amorphous good whose discovery and extraction can be engineered through new technologies. And for self-tracking, too, it is this datafication – the conversion to 'formal' material – that is at the crux of the promise of technological objectivity (also see Steyerl 2016).

In short, self-tracking discourse leverages the historically accumulated virtues of objectivity and technology in order to buttress a vision of neutral optimisation and data-driven truth. Alongside its positioning in the broader (and utopian) history of personal computing, self-tracking discourse's parasitic and derivative relationship to these older values allow them to invest a great deal of transformative capacity in the tracking machines of the present (and the allegedly-near future). In other words, self-tracking not only *repeats* earlier waves of hyperbole surrounding new technologies from electricity to the Internet, it deliberately *reproduces* it as part of its bid for social significance and public uptake. Of course, such promises of technological transformation are rarely fulfilled in exactly the ways foreseen by its pioneers. Self-tracking is unlikely to eliminate uncertainty in self-knowledge any more than mechanical objectivity could eradicate the scientist from science. And so,

we may look forward to a time when today's 'new media', filled with such hopes and fears, itself becomes the stepping stone for the next sociotechnical revelation; as if this time, the Hegelian dialectic will come to a conclusion, and pure objectivity might finally be at hand. We may repeat what we have said of data-sense: honeymoon objectivity is no prophecy, but works very much in the present, legitimising new power relations and systems of veridical authority demanded by new technological practices.

OF FORKING PATHS

The promise of self-tracking is outwardly a simple one: use new technologies to know yourself better. Undergirding this smooth narrative, and lending it a historically accumulated veridical authority, are old and venerable regulative ideals, themselves knitted together into mutually amplify their legitimacy. Insofar as the values of technology, objectivity, and 'raw' data pass themselves off as 'givens', they attempt to depict the human adoption of data-sense as natural and inevitable. Yet when we peel away the presentist fantasies of the revolution that always seems just around the corner, it is possible to understand data-sense not as an 'upgrade', but a question for the subjects of data-driven surveillance: what kind of *relationship* will we broker with this technology, with what kind of consequences? What are the many

paths that are available for those who live in the midst of 'new' technologies, especially if their deployment in some form often seems irresistible?

In 2014, a design consultant named Dan Saffer wrote for *Wired* to make the point rather creatively: we need to tame our algorithms, he argued, like humans tamed animals (Saffer 2014). As we domesticated wolves into dogs, we also evolved to render ourselves compatible with them; the same must now happen, Saffer suggested, with a nonhuman 'species' that we have let loose into our lived environments – algorithms. Saffer's jaunt into this von Uexküllian – not to mention Deleuzian – territory exemplifies a minoritarian discourse within self-tracking that has begun to question what *different* kinds of data-sense might be possible. If self-tracking's sceptics, as we saw in Chapter 2, tended to revert to a binary between pre-technical humanity and a cyborg abomination, commentary like Saffer's attempts to consider ways in which self-tracking might not present society with a set of choices about the virtues it could embrace:

> One way of speeding up this evolution [of humans and algorithms] is providing a means of telling [algorithms] what we need and value. We need to insert an awareness of human feelings and human limitations into the code.

I will end by raising one further example. Perhaps the best known critic of self-tracking as a relationship is, ironically, also one of its iconic practitioners. In the early 2010s, Chris Dancy's apparatus of "between 300 and 700 tracking and lifelogging systems at all times" (Kelly 2014) earned him the label 'the most connected man on earth'. Since then, he has maintained his involvement in the practice, but as a strong proponent of self-tracking as an aid to 'nonjudgmental living'.

> We have a choice when we design software to […] design for contemplation, to design for perspective. Perspective should be a platform […] it's ironic that your phones are fully charged, and you're constantly worried about how far you are away from an outlet, but *you* are worn out, you get no sleep […] if you cared for you as much as you cared for your phone, you'd be amazingly happy (Dancy 2015).

Dancy argues that when self-tracking practices seek to organise subjects into the machinic virtues of standardisation, optimisation, and quantification, this risks 'weaponising' the technology (Dancy, 2015, personal communication) – that is, betraying the empowering or liberating possibilities of the new technology and instead subjecting its users to debilitating anxiety. Such criticism reprises the fear of technology that we also found in the 'humanist' sceptics of Chapter 2, and indeed, earlier warnings about sociotechnical systems like the figure of Charlie Chaplin in *Modern Times*: the human

reduced to a biological copy of the machine, toiling each moment to keep the numbers afloat. More significant is the point of intersection between Dancy's complaint and the earlier example of 'training' algorithms: an emphasis on the possibility, and indeed, *responsibility*, to redirect the developing relationship between self-tracking and the subjective virtues it becomes conduit for. At a moment when the tinkerers' hopes of technological empowerment in the Quantified Self movement is being overwhelmed by the fast-growing commercial interest in consumerist/technological solutionism and looks forward to an economy based on the harvesting of yet more personal data, these kinds of concerns reflect the acute need for a wider public conversation about what how these new technologies are understood, and what fantasies of objectivity, progress and 'raw data' they subscribe to. Data epistemology is a moral question, and insofar as it is socially engineered, a political question.

These concerns over the human-machine relationship thus reflect the seductive danger of honeymoon objectivity. In the latter, the authoritative force of machinic sensibility and epistemic certainty threatens to evacuate the discursive space for public reflection on the biases of data-driven knowledge. After all, if technology delivers a 'neutral' objectivity, what need is there for

philosophical, critical-theoretical, and moral regulation? (see boyd & Crawford 2012, p666) Gilbert Simondon's work shows that the instrumental dream of technology actually *minorises* technology, downplaying and concealing its influence and stakes (see Hörl 2015). The insistent invocations of 'raw data' constantly publicises a technological fantasy of something pure, untainted, but also something that reduces and standardises every kind of phenomenon to a countable and recordable mass. What is at stake in self-tracking's fantasies of 'better knowledge' is precisely this opportunity to cultivate a relationship with technology that is not reducible to the old modernist projects of progress and objectivity.

Postscript.

The present work sought to understand the advent of new surveillance technologies in early twenty-first century America in epistemic terms; that is, a social and political struggle over accepted forms of producing and validating 'knowledge'. It has tried to show how claims to knowledge are so often intertwined with projections of uncertainties and unknowns, analogous to the ways in which identity is defined through its Others. The objects, material and figurative, whose social life we have traced – from recessive objects (Chapter 1) to 'raw' data (4), from the objective 'me' (2) to the invocation of risk (3) – are sites where the production of knowns and unknowns intersect, and through which actors seek to establish desired epistemic configurations. Throughout, I have argued that uncertainty – as distinct from claims to knowledge, and from rationalised forms like risk – is subject to production and management as much as its more positive counterparts, and deserving of further analysis in those terms. I also sought to depict electronic surveillance in terms that are compatible with, but distinct from, the currently dominant frames of security and privacy, control and emancipation. This was not to deny the importance of the latter, but to provide another kind of analytical lens – one which examines the wider

public debate, organised through broad imaginaries of terrorism, technology, posthumanism, self-optimisation.

In the Introduction, I suggested that the Snowden Affair and the Quantified Self constitute two emergent sites for the ongoing efforts to datafy the world around us through new surveillance technologies. These cases tell two parallel aspects of the same, larger story; they share and perpetuate fundamental fantasies about technological progress and objective knowledge, about the steady colonisation of the world through calculation, about the primacy of machinic sensibility, about the mythical figure of 'raw' data. Yet within this larger story, there are differences. While driven by technological inventions and procedures, the data epistemologies they seek to deploy is a social and political process by which veridical authority over the 'self' is transferred, distributed, bureaucratised, sold for consumption. As surveillance technology and data hunger encounters different interests and affordances at social, political, material, institutional, economic levels, we find varying distributions of epistemic authority across state and self-surveillance. Where the former derives its legitimacy against the projected uncertainty of New Terrorism, the latter plays itself up through the tropes of liberal freedoms and posthumanist evolution. Where one plays out through the

consumer market, the other does so through secret and invisibilised circuits of adoption and deployment.

These differences help us think through the less visible dimensions and possibilities latent in each context. Debates on surveillance are typically parsed through the frames of privacy, control and top-down power. In this light, self-surveillance has been able to present itself as an emancipatory endeavour. Just as critics of corporate data-mining call for allowing individuals to 'own' their data and to know 'transparently' how it is being used, the spectre of the rational, informed individual holds together the idea that subjects can take charge of their own datafication to know, improve and control themselves. Yet the perils of voluntary self-datafication in the tracking context demonstrates how surveillance is not simply a problem of ownership and transparency. Rather, it is a question of what epistemic processes and standards gain the right to speak for the self. Conversely, the heuristics and simulations in play vis-à-vis state surveillance disrupt the simple narrative of technological evolution towards objectivity, and draw attention to the institutionalisation of epistemic processes that are marketed to be the epitome of personalisation. To be sure, there is a clear difference between surveillance that no ordinary citizen has any say over, and one that depends on voluntary

engagement through consumption. One lines the edges of everyday experience and knowability, while the other saturates it. But it is not so simple as saying that one is forced and the another is voluntary, that one can be known and the other cannot, or even that 'knowing' and 'having' my own data always amounts to control over the epistemic process. The entanglement of surveillance and uncertainty is about establishing sociotechnical systems whereby the ordinary subject – the citizen, the consumer, member of the 'public' – becomes the ingredient, the raw material, the object, the target, for the production of truths and judgments about themselves.

The concepts raised across the four chapters pin down key aspects of such a process. *Recessive objects* (Chapter 1) demonstrate how information and certainty are not necessary couplings, and how the social presence of things – whether potential, remote, secret, speculative – drives their distribution and problematisation in the epistemic register. The presentation of apparent 'facts' and 'realities' – from the evidence of dragnets to the advent of New Terrorism, from the figure of 'raw' data to the promise of data's intimacy – modulates the boundaries and standards governing what is considered knowable, unknowable, must-be-known, negligible, random, predictable. For new surveillance technologies, the basic assertion underlying its particular

configuration of knowledge and uncertainty is the primacy of *machinic sensibility* (Chapters 1, 2). Within this broader frame of data-driven knowledge, we see how practical strategies are developed in the form of deferring and simulating *heuristics* (Chapter 3), and rationalised through the old modernist imaginaries – in particular, of a *honeymoon objectivity* (Chapter 4). If heuristics like subjunctivity and interpassivity are the everyday practices through which we navigate the presence of uncertainties (a presence itself generated through surveillance discourse), then fantasies like honeymoon objectivity provide a trajectory that justifies collective investment in such imperfect technologies and speculative processes. Although each concept is introduced here through specific phenomena belonging to one of the two empirical cases, when knitted together, they reflect the broader trends in datafication and the corresponding redistribution of epistemic authority in the 'new' media society.

And so, there is much more to be said. It is perhaps the fate of any scholarly endeavour to paint its own boundaries – and the lines of flight it hopes the readers will take up – as much as what it can adequately claim to have addressed. To conclude, I briefly sketch out the boundaries of the present

work: the central questions it raises, the fundamental problems which it sought to address in its own partial and specific way.

***

John Durham Peters (2015) once said that "all recorded media enable an interaction between the living and the dead." New media technologies don't just connect us to each other, but also to nonexistent Others, to imagined strangers, to black-boxed machinic systems, to secrets nestled deep within the unknown and unknowable. The fantasies of knowing the other, knowing through others, knowing the self through machines, beget – and are themselves concretised – through new technologies and their attendant rhetoric. But just as electricity could not fulfil the hopes of erasing temporal and spatial distance (Marvin 1988; Peters 1999), and the Internet did not exactly 'overthrow matter'[103] in a 'Digital Revolution' (the term aired in the inaugural issue of *Wired* claimed), data-driven surveillance is hardly the arrival of clean, machinic objectivity. Instead, we might think of these claims

[103] 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age' (Dyson et al. 1994), a manifesto whose writers included the futurist Alvin Toffler, not only dovetailed with the wider utopian visions of the Internet, but also translated – via Newt Gingrich, in attendance at the conference that birthed the document – into a state policy of deregulation (Turner 1996, Chapter 7).

as part of a game of musical chairs in the regimes of knowledge: a social redistribution of what is considered known/knowable (or not), who (or what) does the knowing, what kind of veridical authority is granted the subject. Peters, responding to an early rendition of the present work, suggested: so much of the world has always been phenomenologically inaccessible to the human subject, before and after modern technology. Yet at each point, what changes is the specific "allocation of ignorance" – and the corresponding relations of power and veridical authority (2015, personal communication).

To claim something is 'known', 'proven', 'revealed', is a powerful speech act; it establishes the referent material as a given upon which other decisions, rationales, truth claims, can be built. And when technologies, institutions, and social norms converge upon a regular system of knowledge claims, this organises a corresponding set of subject positions and the labour they are motivated towards. When the promise of surveillance knowledge hits claims about the unpredictability of New Terrorism like hammer and anvil, the pressure point is the political clamour for 'zero tolerance' on terrorism; and it is such pressure that yields what we have called *fabrication* (Chapter 3), whereby the ambiguous mental and social struggles of certain American youths are reified into signs of the enemy. When trackers like Thync and

Muse promise to resolve the amorphous experiences of 'energy' or 'calm' through the twenty-first century magic of sensor technologies (Chapter 2), they similarly seek a society where subjects' everyday life is organised by micro-scale quantification and best behaviour as dictated by the numbers. While neither strategy is intended by its practitioners to be absolutely exhaustive, they indicate the ways in which new standards for declaring the truth of individuals may emerge. The stakes of fantasies about technology and knowledge thus concern what kinds of acts, beliefs, dependencies, formal standards, subjects are enrolled into in the name of better knowledge.

***

In "A Cyborg Manifesto" (1991), Donna Haraway writes: "our best machines are made of sunshine; they are all light and clean", or rather, they are often *believed to be*. Surveillance technologies are today wired into 'clouds' – a term which names as much the expanding network of machines hidden from ordinary human perception as much as the collective fantasy of a smooth and ethereal connectivity (Hu 2015). This imaginary corresponds to the fantasies of 'pure' and frictionless knowledge, emblematised in the mythical object that we call 'raw data' (Chapter 4). As old (and so often criticised) as they are, the

ideals of objective knowledge and technological progress continue to operate as the 'givens' of new claims about new technologies – from the 'collect 'em all' strategies of state surveillance systems (Chapter 1), to the attempts at measuring and quantifying sleep, sex, and everything in-between (Chapter 2). Unravelling these knotted claims upon which surveillance asserts its validity is to ask: what do people mean by objectivity, by technology, by knowledge, in this context? And what other kinds of social significance could surveillance technologies have, if they were not bound up by this dominant narrative?

Here, we might make an ironic usage of none other than Kevin Kelly's discourse. In a book titled 'What Technology Wants' (2010), Kelly insists that technology has inbuilt tendencies towards perpetual progress. Yet he also provides a rather different way of thinking in his observations of the Amish. Kelly explains that in the communities he visited, technology was not banned outright; instead, enthusiastic early adopters might make a case for a specific object to the community, after which they would be permitted to use it for a trial period. Having carefully observed its impact on everything from the adopter's social life to daily habits, the elders would make a ruling. Contemporary America writ large has no such pilot test. It simply asks: is it technologically feasible? And can the public be seduced into buying it? The

public presentation of surveillance technologies reify this reductive picture of the meaning of technology, where the value and meaning of technologies are defined by criteria like accuracy and efficiency. Honeymoon objectivity is a direct consequence of such 'minorising' of technology – the reduction of technology to mere instrument (see Hörl 2015). As the very concept of technology has grown into an enormous sprawl, covering seemingly every imaginable human work, our resources for thinking and talking about it have often been *narrowed*.

Scholars of technology have variously attempted to address this problem. Andrew Feenberg (1991) wrote of 'another technology': that the question is not whether a given technology is good or bad, but how the objects and processes in question can be turned into a different set of virtues and ideals. More practically, the influential philosopher of existential risk Nick Bostrom (2002) has suggested institutionalising 'differential' technological development; a distribution of monetary incentives by which, as the Amish attempt, more holistic and moral standards can be used to accelerate or slow the development of new technologies.

Yet the problem may run deeper, towards the very concept of 'technology' as an object for thinking and categorising. Since its modern inception in the 1840s, technology has described – and in doing so, reified – the idea that mechanical inventions are expanding quickly and constantly; that they colonise each aspect of human life they touch with a consistent set of principles, from temporal regularity to quantification. Honeymoon objectivity, of course, is itself a truth-claim, one which is then taken as a given by secondary assertions and decisions. The cultural capital commanded by the modern concept of technology thus undergirds surveillance's claims to technological solutionism – even as individual tracking devices often splutter and fail at providing genuine 'insights', and vast, costly state surveillance apparatuses struggle to point to concrete evidence of their efficacy. To speak of knowledge and technology is, so often, to bestow present failures and injustices with an aura of inevitable progress and ultimate good. To perceive such struggles clearly, and to truly speak about 'another technology', it may take jettisoning the very word – and the centuries of accumulated conceptual baggage it now serves as carrier for (Carolyn Marvin, 2016, personal communication).

Surveillance, whether of the state or self variety, is unlikely to vanquish uncertainty to any significant degree. What it *is* attempting – and marking some early successes –is establishing new systems for capturing the private activities, personal communications, daily habits – the little spaces which had remained 'free': free from the ordering and organising devices of knowledge production, from the devices by which subjects are turned into things other than what they themselves think, say, and experience. As fantasies of technologically augmented knowledge continue to accrue cultural capital and achieve material deployment, we should regard with suspicion the common sense linkages between knowledge and virtues like empowerment or justice – and critically evaluate the structural changes that are made in the name of better knowing.

References.

INTRODUCTION

Aas KF (2006) 'The body does not lie': Identity, risk and trust in technoculture. *Crime, Media, Culture*, 2, 143–158.

Adey P (2009) Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space*, 27(2), 274–295.

Amoore L and Hall A (2009) Taking people apart: digitised dissection and the body at the border. *Environment and Planning D: Society and Space*, 27(3), 444–464.

Bamford J (2008) *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York, Doubleday.

Bauman Z and Lyon D (2013) *Liquid Surveillance: A Conversation*. Cambridge, Polity.

Boesel WE (2013) What is the Quantified Self Now? *Quantified Self*, Available from: http://quantifiedself.com/2013/05/what-is-the-quantified-self-now/ (accessed 10 May 2016).

Bogard W (1996) *The Simulation of Surveillance: Hyper Control in Telematic Societies*. Cambridge, Cambridge University Press.

Bourdieu P (1984) How Can One Be a Sportsman? In: *Sociology in Question*, London, SAGE, pp. 117–131.

Bourdieu P (1991) Sport and Social Class. In: Mukerji C and Schudson M (eds), *Rethinking Popular Culture: Contemporary Perspectives in Cultural Studies*, Berkeley, University of California Press, pp. 357–372.

Bucher T (2012) Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, 14(7), 1164–1180.

Butterfield AD (2012) *Quantified Self Meetup Group Assessment*. Available from: http://quantifiedself.com/wp-content/uploads/2012/04/QS-Meetup-Assessment-final-version-1.pdf.

Cohen JE (2013) What Privacy Is For. *Harvard Law Review*, 126, 1904–1933.

Creasey S (2014) Wearable technology will up the game for sports data analytics. *ComputerWeekly*, Available from: http://www.computerweekly.com/feature/Wearable-technology-will-up-the-game-for-sports-data-analytics (accessed 14 April 2016).

Derrida J (1998) *Archive Fever: A Freudian Impression*. Chicago, Chicago University Press.

Diffie W and Landau S (1999) *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MIT Press.

Fitbit Reports $712M Q415 and $1.86B FY15 Revenue; Guides to $2.4 to $2.5B Revenue in FY16 (2016) *Fitbit*, Available from: https://investor.fitbit.com/press/press-releases/press-release-details/2016/Fitbit-

Reports-712M-Q415-and-186B-FY15-Revenue-Guides-to-24-to-25B-Revenue-in-FY16/default.aspx (accessed 13 May 2016).
Foucault M (1995) *Discipline and Punish: The Birth of the Prison*. New York, Vintage Books.
Gandy O (1993) *The panoptic sort: A political economy of personal information*. Boulder, Westview Press.
Gates KA (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York, New York University Press.
Giddens A (1990) *The Consequences of Modernity*. Cambridge, Polity Press.
Gill R and Pratt A (2008) In the Social Factory? Immaterial Labour, Precariousness and Cultural Work. *Theory, Culture & Society*, 25(7-8), 1–30.
Giorgi G (2013) Improper Selves: Cultures of Precarity. *Social Text*, Duke University Press, 31(2 115), 69–81.
Gillespie T (2010) The politics of 'platforms'. *New Media & Society*, 12(3), 347–364.
Gillespie T (2014) The Relevance of Algorithms. In: Gillespie T, Boczkowski PJ, and Foot KA (eds), *Media Technologies: Essays on Communication, Materiality, and Society*, Cambridge, MIT Press, pp. 167–194.
Gitelman L and Jackson V (2013) Introduction. In: Gitelman L (ed.), *Raw Data is an Oxymoron*, Cambridge, MIT Press, pp. 1–14.
Habermas J (1991) *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MIT Press.
Hansen D (2014) Mind-controlled computing: Look, Ma, no hands. *Globe and Mail*, Available from: http://www.theglobeandmail.com/report-on-business/small-business/sb-managing/mind-controlled-computing-look-ma-no-hands/article20948227/ (accessed 28 March 2016).
Kelly K (2011) Self-tracking? You will. *KK*, Available from: http://kk.org/thetechnium/self-tracking-y/ (accessed 10 May 2016).
Kirchner L (2015) When Discrimination Is Baked Into Algorithms. *The Atlantic*, Available from: http://www.theatlantic.com/business/archive/2015/09/discrimination-algorithms-disparate-impact/403969/ (accessed 15 April 2016).
Kittler FA (1986) *Gramophone, Film, Typewriter*. Stanford, Stanford University Press.
Lemov R (2015) *Database of dreams: the lost quest to catalog humanity*. New Haven, Yale University Press.
Leydesdorff L (2000) Luhmann, Habermas and the Theory of Communication. *Systems Research and Behavioral Science*, 17, 273–288.
Mackenzie A (2006) *Cutting Code: Software and Sociality*. New York, Peter Lang.
Mattelart A (2010) *The Globalization of Surveillance: The Origin of the Securitarian Order*. Cambridge, Polity Press.
Mayer J (2006) The Hidden Power. *The New Yorker*, Available from: http://www.newyorker.com/magazine/2006/07/03/the-hidden-power (accessed 10 May 2016).
Medosch A (1997) Interview with Gary Wolf, Wired Digital. *Telepolis*, Available from: http://www.heise.de/tp/artikel/3/3107/1.html (accessed 10 May 2016).

Murphie A (2015) The World as Medium - Whitehead's Media Theory. In: *Affect Theory Conference | Worldings | Tensions | Futures*, Lancaster, PA.
Nakashima E and Warrick J (2013) For NSA chief, terrorist threat drives passion to 'collect it all'. *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (accessed 15 February 2016).
Neilson B and Rossiter N (2008) Precarity as a Political Concept, or, Fordism as Exception. *Theory, Culture & Society*, 25(7-8), 51–72.
Parks L (2007) Points of Departure: The Culture of US Airport Screening. *Journal of Visual Culture*, 6(2), 183–200.
Poster M (1995) Databases as Discourse, or Electronic Interpellations. In: *The second media age*, Cambridge, Polity Press, pp. 78–94.
Ramirez E (2015) QS Access: Personal Data Freedom. *Quantified Self*, Available from: http://quantifiedself.com/2015/02/qs-access-personal-data-freedom/ (accessed 14 April 2016).
Rosenberg D (2013) Data before the Fact. In: Gitelman L (ed.), *Raw Data is an Oxymoron*, Cambridge, MIT Press, pp. 15–40.
Schwarz JA (2015) The Consecration of Information: A Humanist Exegesis of Kopimism. In: *Digital Existence: Memory, Meaning, Vulnerability*, Sigtuna, Sweden.
Shahani A (2012) Who Could Be Watching You Watching Your Figure? Your Boss. *NPR*, Available from: http://www.npr.org/sections/alltechconsidered/2012/12/26/167970303/who-could-be-watching-you-watching-your-figure-your-boss (accessed 14 April 2016).
Shannon CE and Weaver W (1963) *The Mathematical Theory of Communication*. Urbana, University of Illinois Press.
Shin SB and Kim YH (2012) Cloud Face. *Shinseungback Kimyonghun*, Available from: http://ssbkyh.com/works/cloud_face/ (accessed 15 April 2016).
Shin SB and Kim YH (2013) Cat or Human. *Shinseungback Kimyonghun*, Available from: http://ssbkyh.com/works/cat_human/ (accessed 15 April 2016).
Swan M (2012) Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, 1(3), 217–253.
Swan M (2013) The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. *Big Data*, 1(2), 85–99.
United States of Secrets (2014) USA, PBS Frontline.
Vadolas A (2012) The bounced cheques of neoliberal fantasy: Anxiety in times of economic crisis. *Subjectivity*, Nature Publishing Group, 5(4), 355–375.
van Zoonen L (2012) I-Pistemology: Changing truth claims in popular and political culture. *European Journal of Communication*, 27(1), 56–67.
Warner M (2002) *Publics and Counterpublics*. New York, Zone Books.
Watson SM (2013) You Are Your Data. *Slate*, Available from: http://www.slate.com/articles/technology/future_tense/2013/11/quantified_self_self_tracking_data_we_need_a_right_to_use_it.html (accessed 14 April 2016).

Wolf G (2010) QS Show & Tell Tips for Presenters. *Quantified Self*, Available from: http://quantifiedself.com/2010/01/qs-showtell-tips-for-present/ (accessed 1 April 2016).
Wolf G (2016) A Public Infrastructure for Data Access. *Quantified Self*, Available from: http://quantifiedself.com/2016/03/larry-smarr-interview/ (accessed 14 April 2016).
Zimmer M (2008) The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0. *First Monday*, 13(3).

CHAPTER ONE

42 Years for Snowden Docs Release, Free All Now (2016) *Cryptome*, Available from: http://cryptome.org/2013/11/snowden-tally.htm (accessed 16 February 2016).
Akkoc R (2015) Edward Snowden admits to John Oliver: I didn't read all of leaked NSA material. *The Telegraph*, Available from: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11518107/Edward-Snowden-admits-to-John-Oliver-I-didnt-read-all-of-leaked-NSA-material.html (accessed 16 February 2016).
Almasy S (2013) Journalist: Snowden has more documents that could harm U.S. *CNN*, Available from: http://www.cnn.com/2013/07/14/politics/nsa-leak-greenwald/ (accessed 16 February 2016).
American Civil Liberties Union v. James Clapper (2nd Cir., 2015), Available from: http://www.ca2.uscourts.gov/decisions/isysquery/68d6af38-9e01-4d88-8d6a-2250f6c8f927/5/doc/14-42_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/68d6af38-9e01-4d88-8d6a-2250f6c8f927/5/hilite/
American Civil Liberties Union v. National Security Agency 493 F.3d 644 (E.D. Mich., 2007), Available from: https://www.aclu.org/files/pdfs/safefree/nsamemo.opinion.judge.taylor.081706.pdf
American Civil Liberties Union v. National Security Agency 493 F.3d 644 (6th Cir., 2007), Available from: http://www.ca6.uscourts.gov/opinions.pdf/07a0253p-06.pdf
Angwin J (2014) *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York, Times Books.
Annual Open Hearing On Current And Projected National Security Threats To The United States (2014) *U.S. Senate Select Committee on Intelligence*, Washington D.C., Available from: http://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-against-united-states#.
Bakker E and de Graaf B (2010) *Lone wolves: how to prevent this phenomenon? Expert Meeting Lone Wolves*. International Centre for Counter-Terrorism – The Hague.
Bamford J (2008) *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York, Doubleday.

Bannister F and Connolly R (2011) The Trouble with Transparency: A Critical Review of Openness in e-Government. *Policy & Internet*, 3(1), 158–187, Available from: http://doi.wiley.com/10.2202/1944-2866.1076.

Bell E, Abramson J, Gibson J, et al. (2014) Journalism After Snowden. In: *Journalism After Snowden*, New York, Available from: http://www.journalism.columbia.edu/event/901/14.

Benjamin W (2009) *The origin of German tragic drama*. London: Verso.

Berlant L and Greenwald J (2012) Affect in the End Times: A Conversation with Lauren Berlant. *Qui Parle: Critical Humanities and Social Sciences*, 20(2), 71–89.

Borges JL (1998) The Library of Babel. In: *Jorge Luis Borges: Collected Fictions*, New York, Penguin Books, pp. 112–118.

Borland J (2013) Glenn Greenwald: 'A Lot' More NSA Documents to Come. *Wired*, Available from: http://www.wired.com/2013/12/greenwald-lot-nsa-documents-come/ (accessed 16 February 2016).

Boyd D and Crawford K (2012) Critical Questions for Big Data. *Information, Communication & Society*, 15(5), 662–679, Available from: http://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878 (accessed 10 November 2013).

Brynielsson J, Horndahl A, Johansson F, et al. (2012) Analysis of weak signals for detecting lone wolf terrorists. *Security Informatics*, 197–204.

Burton F and Stewart S (2008) The 'Lone Wolf' Disconnect. *STRATFOR*, Available from: https://www.stratfor.com/weekly/lone_wolf_disconnect (accessed 20 February 2016).

Butler J (1997) *The Psychic Life of Power*. Stanford, Stanford University Press.

Carlucci J and LaGanke B (2015) *Drone Boning*. Film. USA, Available from: http://www.droneboning.com/.

Cauley L (2006) NSA has massive database of Americans' phone calls. *USA Today*, Available from: http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm (accessed 14 February 2016).

Chappell B (2013) The Tsarnaev Brothers: What We Know About The Boston Bombing Suspects. *NPR*, Available from: http://www.npr.org/sections/thetwo-way/2013/04/20/178112198/the-tsarnaev-brothers-what-we-know-about-the-boston-bombing-suspects (accessed 20 February 2016).

Clarke RA, Morell MJ, Stone GR, et al. (2013) *Liberty and Security in a Changing World*. Available from: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Coffey S, Wen P and Carroll M (2013) Bombing suspect spent Wednesday as typical student. *Boston Globe*, Available from: https://www.bostonglobe.com/metro/2013/04/19/bombing-suspect-attended-umass-dartmouth-prompting-school-closure-college-friend-shocked-charge-boston-marathon-bomber/8gbczia4qBiWMAP0SQhViO/story.html (accessed 20 February 2016).

Cohen T (2014) Military spy chief: Have to assume Russia knows U.S. secrets. *CNN*, Available from: http://www.cnn.com/2014/03/07/politics/snowden-leaks-russia/ (accessed 16 February 2016).

Cole M and Windrem R (2013) How much did Snowden take? At least three times number reported. *NBC News*, Available from: http://www.nbcnews.com/news/other/how-much-did-snowden-take-least-three-times-number-reported-f8C11038702 (accessed 16 February 2016).

Crawford J (2015) Top intel official: Edward Snowden forced 'needed transparency'. *CNN*, Available from: http://www.cnn.com/2015/09/09/politics/james-clapper-edward-snowden-transparency/ (accessed 16 February 2016).

Dahlberg L (2007) Rethinking the fragmentation of the cyberpublic: from consensus to contestation. *New Media & Society*, 9(5), 827–847.

Davidson A (2004) Introduction. In: Foucault M (2004) *Abnormal: Lectures at the College de France 1974-1975*, New York, Picador.

Debord G (1990) *Comments on the Society of the Spectacle*. London, Verso.

Doyle AC (2005) *The Sign of the Four*. Stilwell, Digireads.com.

Dzhokhar and Tamerlan: A Profile of the Tsarnaev Brothers (2013) *CBS News*, Available from: http://www.cbsnews.com/news/dzhokhar-and-tamerlan-a-profile-of-the-tsarnaev-brothers/ (accessed 20 February 2016).

Eby CA (2012) The Nation That Cried Lone Wolf: A Data-Driven Analysis of Individual Terrorists in the United States Since 9/11. Naval Postgraduate School.

Edward Snowden admits he didn't read all top-secret leaked documents (2015) *One News*, Available from: https://www.tvnz.co.nz/one-news/world/edward-snowden-admits-he-didn-t-read-all-top-secret-leaked-documents-6278317 (accessed 16 February 2016).

Edward Snowden: Whistleblower or double agent? (2013) *Fox News*, Available from: http://www.foxnews.com/politics/2013/06/14/edward-snowden-whistleblower-or-double-agent.html (accessed 16 February 2016).

Eisler P and Page S (2013) 3 NSA veterans speak out on whistle-blower: We told you so. *USA Today*, Available from: http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/ (accessed 15 February 2016).

Fantz A (2013) NSA leaker ignites global debate: hero or traitor? *CNN*, Available from: http://www.cnn.com/2013/06/10/us/snowden-leaker-reaction/ (accessed 16 February 2016).

Farivar C (2013) Snowden distributed encrypted copies of NSA files across the world. *Wired*, Available from: http://www.wired.co.uk/news/archive/2013-06/26/edward-snowden-nsa-data-copies (accessed 16 February 2016).

Fleck L (1979) *Genesis and Development of a Scientific Fact*. Trenn TJ and Merton RK (eds), Chicago, University of Chicago Press.

Foucault M (1972) *The Archaeology of Knowledge*. New York, Pantheon Books.

Foucault M (1995) *Discipline and Punish: The Birth of the Prison*. New York, Vintage Books.

Foucault M (2002) *The Order of Things: An archaeology of the human sciences*. London: Routledge.

Foucault M (2003) *Society Must Be Defended: Lectures at the Collège de France, 1975-1976*. Basingstoke, Palgrave Macmillan.

Foucault M (2006) *Psychiatric Power: Lectures at the Collège de France, 1973-74*. Basingstoke, Palgrave Macmillan.

Foucault M (2008) *The Birth of Biopolitics: Lectures at the Collége de France, 1978-79*. Basingstoke: Palgrave Macmillan.

Foucault M (2014) *On The Government of the Living: Lectures at the Collège de France, 1979-1980*. Basingstoke, Palgrave Macmillan.

Fields G and Perez E (2009) FBI Seeks to Target Lone Extremists. *The Wall Street Journal*, Available from: http://www.wsj.com/articles/SB124501849215613523 (accessed 9 May 2016).

Freedman C (1984) Towards a Theory of Paranoia: The Science Fiction of Philip K. Dick. *Science Fiction Studies*, 11(1), 15–24.

Frers L (2013) The matter of absence. *Cultural Geographies*, 20(4), 431–445.

Friedersdorf C (2015) Why Did It Take the Pentagon a Month to Figure Out Its Files Were Compromised? *The Atlantic*, Available from: http://www.theatlantic.com/politics/archive/2015/06/why-did-it-take-the-pentagon-a-month-to-figure-out-its-files-were-compromised/394991/ (accessed 16 February 2016).

Froomkin D (2015) The Computers Are Listening. *The Intercept*, Available from: https://theintercept.com/2015/05/05/nsa-speech-recognition-snowden-searchable-text/ (accessed 16 February 2016).

Galison P (2008) Removing Knowledge: The Logic of Modern Censorship. In: Procter RN and Schiebinger L (eds), *Agnotology: The Making & Unmaking of Ignorance*, Stanford, Stanford University Press, pp. 37–54.

Gallagher R (2013) Latest Documents From Snowden Provide Direct Proof of Unlawful Spying on Americans. *Slate*, Available from: http://www.slate.com/blogs/future_tense/2013/08/16/latest_snowden_documents_prove_proof_of_unlawful_spying_on_americans.html (accessed 15 February 2016).

Gates KA (2013) The cultural labor of surveillance: video forensics, computational objectivity, and the production of visual evidence. *Social Semiotics*, 23(2), 242–260.

Gates KA (2015) Big Data and State Transparency: What the Absence of Data on Police Killings Reveals. In: *Democracy, Citizenship and Constitutionalism*, Philadelphia, Available from: https://www.sas.upenn.edu/dcc/event/kelly-gates.

Gellman B (2013) Edward Snowden, after months of NSA revelations, says his mission's accomplished. *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html (accessed 15 February 2016).

Gellman B and DeLong M (2013a) The NSA's problem? Too much data. *The Washington Post*, Available from:

http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/ (accessed 16 February 2016).

Gellman B and DeLong M (2013b) What to say, and not to say, to 'our overseers'. *The Washington Post*, Available from: http://apps.washingtonpost.com/g/page/national/what-to-say-and-not-to-say-to-our-overseers/390/?hpid=z2#document/p1/a115513 (accessed 20 February 2016).

Gellman B, Blake A and Miller G (2013) Edward Snowden comes forward as source of NSA leaks. *The Washington Post*, Available from: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html (accessed 15 February 2016).

Gerecht RM (2013) The Costs and Benefits of the NSA. *The Weekly Standard*, Available from: http://www.weeklystandard.com/article/costs-and-benefits-nsa/735246 (accessed 16 February 2016).

Gill P, Horgan J and Deckert P (2014) Bombing alone: tracing the motivations and antecedent behaviors of lone-actor terrorists. *Journal of forensic sciences*, 59(2), 425–35.

Goffman A (2014) *On the Run: Fugitive Life in an American City*. Chicago, University of Chicago Press.

Goldman A (2013) The NSA Has No Idea How Much Data Edward Snowden Took Because He Covered His Digital Tracks. *Business Insider*, Available from: http://www.businessinsider.com/edward-snowden-covered-tracks-2013-8 (accessed 16 February 2016).

Greenwald G (2013a) NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, Available from: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed 14 February 2016).

Greenwald G (2013b) US orders phone firm to hand over data on millions of calls. *The Guardian*, London, 6th June.

Greenwald G (2014) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London, Penguin Books.

Greenwald G (2015) The Sunday Times' Snowden Story is Journalism at its Worst — and Filled with Falsehoods. *The Intercept*, Available from: https://theintercept.com/2015/06/14/sunday-times-report-snowden-files-journalism-worst-also-filled-falsehoods/ (accessed 16 February 2016).

Hacking I (1990) *The Taming of Chance*. Cambridge, Cambridge University Press.

Hansen MBN (2015) *Feed-Forward: On the Future of Twenty-First-Century Media*. Chicago, University of Chicago Press.

Haraway D (1991) A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century. In: *Simians, Cyborgs and Women: The Reinvention of Nature*, New York, Routledge, pp. 149–181.

Harman G (2002) *Tool-Being: Heidegger and the Metaphysics of Objects*. Peru, Illinois, Open Court.

Harris S (2010) *The Watchers: The Rise of America's Surveillance State*. New York, The Penguin Press.
Heidegger M (1962) *Being and Time*. New York, Harper & Row.
Henderson B (2013) Boston Marathon bombs: suspect captured - April 20 as it happened. *The Telegraph*, Available from: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10007370/Boston-Marathon-bombs-suspect-captured-April-20-as-it-happened.html (accessed 20 February 2016).
Hill E (2002) *Joint Inquiry Staff Statement, Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001*. Available from: http://fas.org/irp/congress/2002_hr/100802hill.html.
Hill K (2013) Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government. *Forbes*, Available from: http://www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/#3528a9b16d06 (accessed 16 February 2016).
Hofstadter R (1967) The Paranoid Style in American Politics. In: *The Paranoid Style in American Politics and Other Essays*, New York: Vintage Books, pp. 3–40.
Hong S (2015) When Life Mattered: The Politics of the Real in Video Games' Reappropriation of History, Myth, and Ritual. *Games and Culture*, 10(1), 35–56.
Hong S and Allard-Huver F (Forthcoming) Governing governments? Discursive contestations of governmentality in the transparency dispositif. In: Mcilvenny P, Klausen JZ, and Lindegaard LB (eds), *Studies of Discourse and Governmentality. New perspectives and methods*, Amsterdam, John Benjamins.
Hörl E (2015) The technological condition. *Parrhesia*, 22, 1–15.
Hosenball M (2013) NSA chief says Snowden leaked up to 200,000 secret documents. *Reuters*, Available from: http://www.reuters.com/article/us-usa-security-nsa-idUSBRE9AD19B20131114 (accessed 16 February 2016).
Howard A (2015) What Snapchat's Latest Privacy Update Actually Means For You. *The Huffington Post*, Available from: http://www.huffingtonpost.com/entry/snapchat-privacy-update-terms-of-service_us_563786cbe4b063179912fbc6 (accessed 17 February 2016).
If it weren't for Edward Snowden conspiracy theories would still just be 'theories' (2015) *Reddit*, Available from: https://www.reddit.com/r/conspiracy/comments/2z31bh/if_it_werent_for_edward_snowden_conspiracy/ (accessed 16 February 2016).
Interview: Glenn Greenwald (2014) *The Nation*, New Zealand, 3 News, Available from: http://www.newshub.co.nz/tvshows/thenation/interview-glenn-greenwald-2014091311?ref=video#axzz3raerQBJl (accessed 16 February 2016).
Jewel v. National Security Agency 673 F.3d 902 (9th Cir., 2011), Available from: https://cdn.ca9.uscourts.gov/datastore/opinions/2011/12/29/10-15616.pdf
Johnson A (2014) Edward Snowden 'Probably' Not a Russian Spy, New NSA Chief Says. *NBC News*, Available from: http://www.nbcnews.com/storyline/nsa-snooping/edward-snowden-probably-not-russian-spy-new-nsa-chief-says-n121926 (accessed 16 February 2016).

Kaati L and Svenson P (2011) Analysis of competing hypothesis for investigating lone wolf terrorists. In: *European Intelligence and Security Informatics Conference*, pp. 295–299.

Kaczynski A (2014) Former NSA Director On Edward Snowden: 'He's Working For Someone'. *BuzzFeed*, Available from: http://www.buzzfeed.com/andrewkaczynski/former-nsa-director-on-edward-snowden-hes-working-for-someon#.pf97er37p (accessed 16 February 2016).

Kelley MB (2013) The Guardian's Bombshell Revelation About NSA Domestic Spying Is Only The Tip Of The Iceberg. *Business Insider*, Available from: http://www.businessinsider.com/the-impact-of-nsa-domestic-spying-2013-6 (accessed 15 February 2016).

Kelley MB (2014) Snowden Has One Very Important And Potentially Devastating Question To Answer. *Business Insider*, Available from: http://www.businessinsider.com/snowden-and-military-information-2014-3 (accessed 16 February 2016).

Kelley MB (2015) John Oliver just exposed a very big lie surrounding Edward Snowden. *Business Insider*, Available from: http://www.businessinsider.com/snowden-and-john-oliver-2015-4 (accessed 16 February 2016).

Kendler KS (1986) Kraepelin and the differential diagnosis of dementia praecox and manic-depressive insanity. *Comprehensive psychiatry*, 27(6), 549–558.

Kendler KS (1988) Kraepelin and the Diagnostic Concept of Paranoia. *Comprehensive Psychiatry*, 29(1), 4–11.

Kittler FA (1986) *Gramophone, Film, Typewriter*. Stanford, Stanford University Press.

Kopstein J (2013) Silicon Valley's Surveillance Cure-All: Transparency. *The New Yorker*, Available from: http://www.newyorker.com/tech/elements/silicon-valleys-surveillance-cure-all-transparency (accessed 16 February 2016).

Krauss LM (2016) Thinking Rationally About Terror. *The New Yorker*, Available from: http://www.newyorker.com/news/news-desk/thinking-rationally-about-terror?intcid=mod-most-popular (accessed 22 February 2016).

Kravets D (2013) NSA Transparency Hurts Americans' Privacy, Feds Say With Straight Face. *Wired*, Available from: http://www.wired.com/2013/11/nsa-transparency-effect/ (accessed 16 February 2016).

Kuhn TS (1962) *The Structure of Scientific Revolutions*. Chicago, University of Chicago Press.

Lake E (2014) Spy Chief: We Should've Told You We Track Your Calls. *The Daily Beast*, Available from: http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html.

Landau S (2013) Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *Spotlight*, (July/August), 54–63.

Last Week Tonight with John Oliver (2015) [Television program] HBO, USA, 5 April. Available from: https://www.youtube.com/watch?v=XEVlyP4_11M.

Ledgett R (2014) The NSA responds to Edward Snowden's TED Talk. *TED 2014*, Available from:

http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk.
Lemov R (2015) *Database of dreams: the lost quest to catalog humanity*. New Haven, Yale University Press.
Leonnig C (2013) Court: Ability to police U.S. spying program limited. *The Washington Post*, Available from: http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html (accessed 1 February 2015).
Leopold J (2015) Inside Washington's Quest to Bring Down Edward Snowden. *Vice News*, Available from: https://news.vice.com/article/exclusive-inside-washingtons-quest-to-bring-down-edward-snowden (accessed 16 February 2016).
Loewenstein A (2014) The ultimate goal of the NSA is total population control. *The Guardian*, Available from: http://www.theguardian.com/commentisfree/2014/jul/11/the-ultimate-goal-of-the-nsa-is-total-population-control (accessed 14 February 2016).
Lone Wolf Tactical Concept (2012) *Aryan Vanguard*, Available from: http://aryanvanguard.blogspot.com/2012/06/lone-wolf-tactical-concept.html (accessed 20 February 2016).
Maass P (2015) Inside NSA, Officials Privately Criticize 'Collect it all' Surveillance. *The Intercept*, Available from: https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/ (accessed 15 February 2016).
Massumi B (2007) Potential Politics and the Primacy of Preemption. *Theory & Event*, 10(2).
McCauley C and Moskalenko S (2014) Toward a Profile of Lone Wolf Terrorists: What Moves an Individual From Radical Opinion to Radical Action. *Terrorism and Political Violence*, 26(1), 69–85.
McDonald A and Cranor LF (2008) The Cost of Reading Privacy Policies. *I/S - A Journal of Law and Policy for the Information Society*, 4(3), 1–22.
McQuillan D (2015) Algorithmic states of exception. *European Journal of Cultural Studies*, 18(4-5), 564–576.
Melley T (2012) *The Covert Sphere: Secrecy, Fiction, and the National Security State*. Ithaca: Cornell University Press.
Merleau-Ponty M (1968) *The Visible and the Invisible*. Lefort C (ed.), Evanston, Northwestern University Press.
Merleau-Ponty M (2012) *Phenomenology of Perception*. London, Routledge.
Michael G (2012) *Lone Wolf Terror and the Rise of Leaderless Resistance*. Nashville: Vanderbilt University Press.
Monahan T (2010) *Surveillance in the Time of Insecurity*. New Brunswick, Rutgers University Press.
Morton T (2013) *Hyperobjects: Philosophy and Ecology after the End of the World*. Minneapolis, University of Minnesota Press.
Nakashima E and Warrick J (2013) For NSA chief, terrorist threat drives passion to 'collect it all'. *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-

threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (accessed 15 February 2016).

National commission on terrorist attacks upon the United States (2004) *The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States: Executive summary*. Available from: http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf

Nørretranders T (1998) *The User Illusion - Cutting Consciousness Down to Size*. New York: Viking.

NSA, other government agencies should be more transparent (2013) *The Washington Post*, Available from: https://www.washingtonpost.com/opinions/nsa-other-government-agencies-should-be-more-transparent/2013/09/15/2041192a-1caf-11e3-8685-5021e0c41964_story.html (accessed 16 February 2016).

Obama B (2009) Memorandum for the Heads of Executive Departments and Agencies: Transparency and Open Government. *The White House*, Available from: https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment (accessed 17 February 2016).

Obama B (2015) Address to the Nation by the President. Available from: https://www.whitehouse.gov/the-press-office/2015/12/06/address-nation-president.

Page S (2006) NSA secret database report triggers fierce debate in Washington. *USA Today*, Available from: http://usatoday30.usatoday.com/news/washington/2006-05-11-nsa-reax_x.htm (accessed 14 February 2016).

Pantucci R (2011) *A Typology of Lone Wolves : Preliminary Analysis of Lone Islamist Terrorists*.

Parikka J (2011) Operative media archaeology: Wolfgang Ernst's materialist media diagrammatics. *Theory, Culture & Society*, 28(5), 52–74.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Harvard University Press.

Pew Research Center (2013) *Majority views NSA Phone Tracking as Acceptable Anti-Terror Tactic*. Available from: http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/.

Pincus W (2013) Questions for Snowden. *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/questions-for-snowden/2013/07/08/d06ee0f8-e428-11e2-80eb-3145e2994a55_story.html (accessed 16 February 2016).

Poindexter J (2002) Information Awareness Office Overview. In: *DARPATech 2002*, Anaheim.

Protecting your Privacy (2015) *Snapchat*, Available from: http://blog.snapchat.com/post/132379796495/protecting-your-privacy (accessed 17 February 2016).

Puar JK and Rai AS (2002) Monster, Terrorist, Fag: The War on Terrorism and the Production of Docile Patriots. *Social Text*, 20(3), 117–148.

Reitman J (2013) Jahar's World. *Rolling Stone*, Available from: http://www.rollingstone.com/culture/news/jahars-world-20130717 (accessed 20 February 2016).

Rich S and DeLong M (2013) NSA slideshow on 'The TOR problem'. *The Washington Post*, Available from: http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/ (accessed 16 February 2016).
Ricoeur P (1967) *Husserl: An Analysis of His Phenomenology*. Evanston, Northwestern University Press.
Rifkin A (2007) *Look*. Film. USA, Captured Films.
Rotman B (2008) *Becoming Beside Ourselves: The Alphabet, Ghosts, and Distributed Human Being*. Pittsburgh, Duke University Press.
Rowan D (2014) Snowden: Big revelations to come, reporting them is not a crime. *Wired*, Available from: http://www.wired.co.uk/news/archive/2014-03/18/snowden-ted.
Rusbridger A (2013) The Snowden Leaks and the Public. *The New York Review of Books*, Available from: http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/ (accessed 16 February 2016).
Russon M-A (2015) Snapchat policy change means it now owns the rights to all your nude photos forever. *International Business Times*, Available from: http://www.ibtimes.co.uk/snapchat-policy-change-means-it-now-owns-rights-all-your-nude-photos-forever-1526481 (accessed 17 February 2016).
Safire W (2002) You Are a Suspect. *The New York Times*, Available from: http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html (accessed 14 February 2016).
Sanchez J (2013) Tech giants named in PRISM want to see an NSA 'transparency report'. *Ars Technica*, Available from: http://arstechnica.com/tech-policy/2013/07/tech-giants-named-in-prism-want-to-see-an-nsa-transparency-report/ (accessed 16 February 2016).
Saury J-M (2008) The phenomenology of negation. *Phenomenology and the Cognitive Sciences*, 8(2), 245–260.
Scarry E (1985) *The Body in Pain: The Making and Unmaking of the World*. Oxford, Oxford University Press.
Schwartz M (2015) The Whole Haystack. *The New Yorker*, Available from: http://www.newyorker.com/magazine/2015/01/26/whole-haystack (accessed 15 February 2015).
Shannon CE and Weaver W (1963) *The Mathematical Theory of Communication*. Urbana, University of Illinois Press.
Sheehan T (2014) *Making Sense of Heidegger: A Paradigm Shift*. London, Rowman & Littlefield International.
Shorrock T (2015) US Intelligence Is More Privatized Than Ever Before. *The Nation*, Available from: http://www.thenation.com/article/us-intelligence-is-more-privatized-than-ever-before/ (accessed 16 February 2016).
Siebers T (1993) *Cold War Criticism and the Politics of Skepticism*. New York, Oxford University Press.
Simon JD (2013) *Lone Wolf Terrorism: Understanding the Growing Threat*. New York, Prometheus Books.

Spaaij R (2012) *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention*. Dordrecht, Springer.
Springer NR (2009) Patterns of Radicalisation: Identifying the Markers and Warning Signs of Domestic Lone Wolf Terrorists in Our Midst. Naval Postgraduate School.
Stevenson D (2004) 'The Gudeman of Ballangeich': rambles in the afterlife of James V. *Folklore*, 115(2), 187–200, Available from: http://www.informaworld.com/openurl?genre=article&doi=10.1080/00155870420002 31273&magic=crossref||D404A21C5BB053405B1A640AFFD44AE3.
Steyerl H (2016) A Sea of Data: Apophenia and Pattern (Mis-)Recognition. *e-flux*, 72, Available from: http://www.e-flux.com/journal/a-sea-of-data-apophenia-and-pattern-mis-recognition/.
Stout M and Goodison D (2013) Dzhokhar Tsarnaev loves pot, wrestling say friends. *Boston Herald*, Available from: http://www.bostonherald.com/news_opinion/local_coverage/2013/04/dzhokhar_tsa rnaev_loves_pot_wrestling_say_friends (accessed 20 February 2016).
Szpunar PM (2015) From the Other to the Double: Identity in Conflict and the Boston Marathon Bombing. *Communication, Culture & Critique*, Early View.
Taussig M (1999) *Defacement - Public Secrecy and the Labour of the Negative*. Stanford: Stanford University Press.
The Art of Saying Nothing (2006) *The New York Times*, Available from: http://www.nytimes.com/2006/02/08/opinion/08wed1.html?_r=0 (accessed 14 February 2016)
Thompson E (2002) *The Soundscape of Modernity: Architectural Acoustics and the Culture of Listening in America, 1900-1933*. Cambridge, MIT Press.
Thrift N (2011) Lifeworld Inc—and what to do about it. *Environment and Planning D: Society and Space*, 29(1), 5–26.
Tom Metzger (n.d.) *Anti-Defamation League*, Available from: http://archive.adl.org/learn/ext_us/tom-metzger/ideology.html?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_ America&xpicked=2&item=7 (accessed 20 February 2016).
US Department of State (1996) *Patterns of Global Terrorism, 1995*. Available from: http://www.hri.org/docs/USSD-Terror/95/.
US Department of State (1997) *1996 Patterns of Global Terrorism Report*. Available from: http://www.state.gov/www/global/terrorism/1996Report/1996index.html.
US Department of State (2000) *Patterns of Global Terrorism 1999*. Available from: http://www.state.gov/www/global/terrorism/1999report/1999index.html.
Utah Data Center (n.d.) *Domestic Surveillance Directorate*, Available from: https://nsa.gov1.info/utah-data-center/ (accessed 22 February 2016).
Vattimo G (1992) *The transparent society*. Baltimore, Johns Hopkins University Press.
Verizon forced to hand over telephone data – full court ruling (2013) *The Guardian*, Available from: https://web.archive.org/web/20130731051526/http://www.theguardian.com/world/i nteractive/2013/jun/06/verizon-telephone-data-court-order (accessed 14 February 2016).

Wensierski P (2015) Web of Surveillance: East German Snitching Went Far Beyond the Stasi. *Der Spiegel*, Available from: http://www.spiegel.de/international/germany/east-german-domestic-surveillance-went-far-beyond-the-stasi-a-1042883.html (accessed 22 February 2016).
Zaret D (2000) *Origins of Democratic Culture: Printing, Petitions, and the Public Sphere in Early-Modern England*. Princeton, Princeton University Press.
Zetter K (2013) Snowden Smuggled Documents From NSA on a Thumb Drive. *Wired*, Available from: http://www.wired.com/2013/06/snowden-thumb-drive/ (accessed 16 February 2016).
Zielinski S (2006) *Deep time of the media: toward an archaeology of hearing and seeing by technical means*. Cambridge, MIT Press.
Žižek S (n.d.) The Interpassive Subject. Available from: http://www.egs.edu/faculty/slavoj-zizek/articles/the-interpassive-subject/.

CHAPTER TWO

Abramson P (2015) Bringing your QS data to the doctor. In: *Quantified Self 2015 Conference*, San Francisco.
Amoore L and Hall A (2009) Taking people apart: digitised dissection and the body at the border. *Environment and Planning D: Society and Space*, 27(3), 444–464.
Anderson J and Rainie L (2014) The Internet of Things Will Thrive by 2025. *Pew Research Center*, Available from: http://www.pewinternet.org/2014/05/14/internet-of-things/ (accessed 28 March 2016).
Athanasius (1987) *Athanasius: Select Works and Letters*. Schaff P and Wace H (eds), New York, Wm. B. Eerdmans Publishing Company.
Beres D (2015) This App Identifies Your Most Toxic Friends. *The Huffington Post*, Available from: http://www.huffingtonpost.com/2015/01/27/pplkpr-identifies-your-worst-friends_n_6554892.html (accessed 31 March 2016).
Berlant L and Edelman L (2014) *Sex, or the Unbearable*. Durham, Duke University Press.
Berlant L and Greenwald J (2012) Affect in the End Times: A Conversation with Lauren Berlant. *Qui Parle: Critical Humanities and Social Sciences*, 20(2), 71–89.
Berry DM (2011) *The Philosophy of Software: Code and Mediation in the Digital Age*. Basingstoke, Palgrave Macmillan.
Bhatt S (2013) We're All Narcissists Now, And That's A Good Thing. *Fast Company*, Available from: http://www.fastcoexist.com/3018382/were-all-narcissists-now-and-thats-a-good-thing (accessed 29 March 2016).
Boltanski L and Chiapello E (2007) *The New Spirit of Capitalism*. London, Verso.
Boyd D and Crawford K (2012) Critical Questions for Big Data. *Information, Communication & Society*, 15(5), 662–679, Available from: http://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878 (accessed 10 November 2013).

Brandon J (2013) 6 Tech Trends of the Far Future. *Inc.*, Available from: http://www.inc.com/john-brandon/6-tech-trends-of-the-far-future.html (accessed 28 March 2016).

Bucher T (2012) Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, 14(7), 1164–1180.

Butterfield AD (2012) *Quantified Self Meetup Group Assessment*. Available from: http://quantifiedself.com/wp-content/uploads/2012/04/QS-Meetup-Assessment-final-version-1.pdf.

Ceglowski M (2015) Haunted by Data. In: *Strata+Hadoop World Conference*, New York, Available from: http://idlewords.com/talks/haunted_by_data.htm.

Chamorro-Premuzic T (2015) Reputation and the rise of the 'rating' society. *The Guardian*, Available from: http://www.theguardian.com/media-network/2015/oct/26/reputation-rating-society-uber-airbnb (accessed 31 March 2016).

Cheney-Lippold J (2011) A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, 28(6), 164–181.

Crawford K, Lingel J and Karppi T (2015) Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies*, 18(4-5), 479–496.

de Brouwer S, Avey L, Richman J, et al. (2015) Frontiers of Tracking Health. In: *Quantified Self 2015 Conference*, San Francisco.

de Certeau M (1984) *The Practice of Everyday Life*. Berkeley, University of California Press.

Dewey C (2015) Everyone you know will be able to rate you on the terrifying 'Yelp for people' — whether you want them to or not. *The Washington Post*, Available from: https://www.washingtonpost.com/news/the-intersect/wp/2015/09/30/everyone-you-know-will-be-able-to-rate-you-on-the-terrifying-yelp-for-people-whether-you-want-them-to-or-not/ (accessed 27 October 2015).

Dougherty N (2013) Quantified/Unquantified: What I've learned from self-tracking in different modes. In: *Quantified Self 2013 Conference*, San Francisco, Available from: http://quantifiedself.com/2014/03/nancy-dougherty-unquantified/.

Elgan M (2012) Is the 'quantified self' movement just a fad? *Computerworld*, Available from: http://www.computerworld.com/article/2499169/enterprise-applications/is-the--quantified-self--movement-just-a-fad-.html (accessed 1 April 2016).

Evans D (2011) The Internet of Things [INFOGRAPHIC]. *CISCO*, Available from: http://blogs.cisco.com/diversity/the-internet-of-things-infographic (accessed 28 March 2016).

Finley K (2013) The Quantified Man: How an Obsolete Tech Guy Rebuilt Himself for the Future. *Wired*, Available from: http://www.wired.com/2013/02/quantified-work/ (accessed 29 March 2016).

Foucault M (1986) *The Care of the Self*. New York, Random House.

Foucault M (1997) *Ethics: Subjectivity and Truth*. Rabinow P (ed.), New York, The New Press.

Foucault M (2001) *Fearless Speech*. Pearson J (ed.), Los Angeles, Semiotext(e).
Foucault M (2004) *Security, Territory, Population: Lectures at the Collège de France 1977-1978*. Senellart M (ed.), New York, Palgrave Macmillan.
Foucault M (2011) *The Courage of Truth: Lectures at the Collège de France, 1983-1984*. Gros F (ed.), Basingstoke, Palgrave Macmillan.
Foucault M (2014a) *On The Government of the Living: Lectures at the Collège de France, 1979-1980*. Basingstoke, Palgrave Macmillan.
Foucault M (2014b) *Wrong-Doing, Truth-Telling: The Function of Avowal in Justice*. Brion F and Harcourt BE (eds), Chicago, University of Chicago Press.
Franklin B (1884) *The Autobiography of Benjamin Franklin*. London, George Bell & Sons, Available from: https://archive.org/stream/autobiographyofb1884fran#page/n8/mode/1up.
Frick L (n.d.) the future of data about you. *LaurieFrick.com*, Available from: http://www.lauriefrick.com/ (accessed 29 March 2016).
Frog (2014) 15 Tech Trends That Will Define 2014, Selected By Frog. *Fast Company*, Available from: http://www.fastcodesign.com/3024464/15-tech-trends-that-will-define-2014-selected-by-frog (accessed 28 March 2016).
Garten A (2011) Know thyself, with a brain scanner. *TED*, Available from: https://www.ted.com/talks/ariel_garten_know_thyself_with_a_brain_scanner/transcript?language=en (accessed 22 June 2012).
Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015 (2015) *Gartner*, Available from: http://www.gartner.com/newsroom/id/3165317 (accessed 28 March 2016).
Gillespie T, Seyfert R and Roberge J (2016) #Trendingistrending: When Algorithms Become Culture. In: *Algorithmic Cultures: Essays on Meaning, Performance and New Technologies*.
Goetz T (2013) The Diabetic's Paradox. *The Atlantic*, Available from: http://www.theatlantic.com/health/archive/2013/04/the-diabetics-paradox/274507/ (accessed 2 April 2016).
Gould SJ (1996) *The Mismeasure of Man: The definitive refutation to the argument of The Bell Curve*. New York, W.W. Norton & Co.
Hacking I (1990) *The Taming of Chance*. Cambridge, Cambridge University Press.
Hansen D (2014) Mind-controlled computing: Look, Ma, no hands. *Globe and Mail*, Available from: http://www.theglobeandmail.com/report-on-business/small-business/sb-managing/mind-controlled-computing-look-ma-no-hands/article20948227/ (accessed 28 March 2016).
Hansen MBN (2015) *Feed-Forward: On the Future of Twenty-First-Century Media*. Chicago, University of Chicago Press.
Havens JC (2014) *Hacking H(app)iness: Why Your Personal Data Counts and How Tracking It Can Change the World*. New York, Jeremy P. Tarcher/Penguin.
Hardaway F (2013) Is Data Porn Good For Anything? *Fast Company*, Available from: http://www.fastcompany.com/3014531/creative-conversations/is-data-porn-good-for-anything (accessed 1 April 2016).

Hardy Q (2013) A Digital Diaper for Tracking Children's Health. *The New York Times*, Available from: http://bits.blogs.nytimes.com/2013/07/09/a-digital-diaper-for-tracking-health/?_r=0&mtrref=undefined&gwh=FBAC46CF55432A6D878C473650CDDDB0&gwt=pay (accessed 29 March 2016).

Hernandez D (2012) Big Data Is Transforming Healthcare. *Wired*, Available from: http://www.wired.com/2012/10/big-data-is-transforming-healthcare/ (accessed 29 March 2016).

Hesse M (2008) Bytes of Life. *The Washington Post*, Available from: http://www.wired.com/2010/11/mf_qa_ferriss/ (accessed 29 March 2016).

Holland E (2013) Finally, A Better Way For 'Quantified Self' Products To Collect Personal Data. *Fast Company*, Available from: http://www.fastcompany.com/3020212/finally-a-better-way-for-quantified-self-products-to-collect-personal-data (accessed 11 May 2016).

Hu T-H (2015) *The Prehistory of the Cloud*. Cambridge, MIT Press.

Jenkins Jr. HW (2010) Google and the Search for the Future. *The Wall Street Journal*, Available from: http://www.wsj.com/articles/SB10001424052748704901104575423294099527212 (accessed 29 March 2016).

Jordan M and Pfarr N (2014) Forget the Quantified Self. We Need to Build the Quantified Us. *Wired*, Available from: http://www.wired.com/2014/04/forget-the-quantified-self-we-need-to-build-the-quantified-us/ (accessed 29 March 2016).

Kelly K (2007) What is the Quantified Self? *Quantified Self*, Available from: https://web.archive.org/web/20150408202734/http://quantifiedself.com/2007/10/what-is-the-quantifiable-self/ (accessed 29 March 2016).

Kelly K (2011) The Quantifiable Self. *KK*, Available from: http://kk.org/thetechnium/the-quantifiabl/ (accessed 2 April 2016).

Kessler S (2013) Can the Quantififed Self Go Too Far? *Fast Company*, Available from: http://www.fastcompany.com/3015762/bed-bath-and-beyond-where-do-you-draw-the-line-when-it-comes-to-self-quantifying (accessed 1 April 2016).

Khosla V (2015) The Algorithms are Coming. What's at stake? In: *Quantified Self 2015 Conference*, San Francisco.

Kronsberg M (2013) Know Thy Quantified Self. *The Wall Street Journal*, Available from: http://www.wsj.com/articles/SB10001424127887324000704578388680077749540 (accessed 1 April 2016).

Lanier J (2010) *You Are Not A Gadget: A Manifesto*. New York, Alfred A. Knopf.

Lauletta T (2016) We tried Moov's new fitness tracker, a robotic personal trainer for your wrist — here's what we thought. *Business Insider*, Available from: http://www.businessinsider.com/moov-now-fitness-tracker-review-2016-1 (accessed 31 March 2016).

Leppakorpi L (2011) Beddit Presentation. In: *MoneyTalks*, Tampere, Available from: http://www.slideshare.net/TechnopolisOnline/beddit-presentation.

Lorenzini D (2016) Daniele Lorenzini on On the Government of the Living. *13/13: Michel Foucault's College de France Lectures*, Available from: http://blogs.law.columbia.edu/foucault1313/2016/02/07/daniele-lorenzini-on-on-the-government-of-the-living/ (accessed 29 March 2016).

Lupton D (2012) M-health and health promotion: The digital cyborg and surveillance society. *Social Theory & Health*, Nature Publishing Group, 10(3), 229–244.

Lupton D (2013a) Quantifying the body: monitoring and measuring health in the age of mHealth technologies. *Critical Public Health*, 23(4), 393–403.

Lupton D (2013b) Understanding the Human Machine. *IEEE Technology and Society Magazine*, 32(4), 25–30.

Lupton D (2014) Self-tracking cultures: towards a sociology of personal informatics. In: *OzCHI '14: Proceedings of the 26th Australian Computer-Human Interaction Conference: Designing Futures, the Future of Design*, Sydney.

Lupton D (2015) Changing representations of self-tracking. *This Sociological Life*, Available from: https://simplysociology.wordpress.com/2015/03/05/changing-representations-of-self-tracking/ (accessed 1 April 2016).

Lupton D (preprint) You are Your Data: Self-tracking Practices and Concepts of Data. In: Selke S (ed.), *Lifelogging: Theoretical Approaches and Case Studies about Self-tracking*, Springer.

Mackenzie D (2010) Unlocking the language of structured securities. *Financial Times*, Available from: http://www.ft.com/cms/s/0/8127989a-aae3-11df-9e6b-00144feabdc0.html#axzz3w2fTTGpL; (accessed 1 April 2016).

Mallett W (2014) Apps Are Getting All Emotional. *Fast Company*, Available from: http://www.fastcompany.com/3039624/apps-are-getting-all-emotional (accessed 29 March 2016).

Meyer R (2012) How You Turn Music Into Money in 2012 (Spoiler: Mostly iTunes). *The Atlantic*, Available from: http://www.theatlantic.com/technology/archive/2012/08/how-you-turn-music-into-money-in-2012-spoiler-mostly-itunes/260678/ (accessed 11 May 2016).

Milburn T (2015) How My Life Automation System Quantifies My Life. In: *Quantified Self 2015 Conference*, San Francisco.

Morga A (2011) Do You Measure Up? *Fast Company*, Available from: http://www.fastcompany.com/1744571/do-you-measure (accessed 29 March 2016).

Morozov E (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York, Public Affairs.

Mother (n.d.) *sen.se*, Available from: https://sen.se/mother/ (accessed 29 March 2016).

Nafus D and Sherman J (2014) This One Does Not Go Up to 11: The Quantified Self Movement as an Alternative Big Data Practice. *International Journal of Communication*, 8, 1784–1794.

North A (2014) Why You Want an App to Measure Calories but Not Character. *The Washington Post*, Available from: http://op-talk.blogs.nytimes.com/2014/08/26/why-you-want-an-app-to-measure-calories-but-not-character/?_r=1 (accessed 1 April 2016).

Oboler A, Welsh K and Cruz L (2012) The danger of big data: Social media as computational social science. *First Monday*, 17(7).
Olson P (2014) Fitbit Data Now Being Used In The Courtroom. *Forbes*, Available from: http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim (accessed 29 March 2016).
Pasquale F (2015a) Scores of Scores: How Companies Are Reducing Consumers to Single Numbers. *The Atlantic*, Available from: http://www.theatlantic.com/business/archive/2015/10/credit-scores/410350/ (accessed 31 March 2016).
Pasquale F (2015b) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Harvard University Press.
Peeple app for rating human beings causes uproar (2015) *BBC News*, Available from: http://www.bbc.com/news/technology-34415382 (accessed 31 March 2016).
Pilliod E (2005) Ingestion / Pontormo's Diary. *Cabinet*, Available from: http://cabinetmagazine.org/issues/18/pontormosdiary.php.
Plato (1899) Phaedrus. In: *Dialogues of Plato, Volume 1*, New York: Charles Scribner's Sons, pp. 515–586.
Plato (1920) Laches. In: *The Dialogues of Plato, Volume 1*, New York: Random House.
Porter TM (1995) *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton, Princeton University Press.
pplkpr (n.d.) *pplkpr.com*, Available from: http://www.pplkpr.com (accessed 31 March 2016).
Quantified Self (n.d.) *Quantified Self*, Available from: http://quantifiedself.com/ (accessed 29 March 2016).
Reeves D (2015) Frictionless Tracking with Beeminder Autodata. In: *Quantified Self 2015 Conference*, San Francisco.
Rettberg JW (2014) *Seeing Ourselves Through Technology: How We Use Selfies, Blogs and Wearable Devices To See and Shape Ourselves*. Basingstoke, Palgrave Macmillan.
Rohling G (2015) Facts and Forecasts: Billions of Things, Trillions of Dollars. *Siemens*, Available from: http://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/internet-of-things-facts-and-forecasts.html (accessed 28 March 2016).
Ruppert E (2011) Population Objects: Interpassive Subjects. *Sociology*, 45(2), 218–233.
Ryan SE (2014) *Garments of Paradise: Wearable Discourse in the Digital Age*. Cambridge, MIT Press.
Scott JC (1998) *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, Yale University Press.
Seneca LA (2012) *Minor Dialogs Together with the Dialog 'On Clemency'*. London, Forgotten Books.
Sharon T (2016) Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. *Philosophy & Technology*, 1–29.
Singer N (2015) Technology That Prods You to Take Action, Not Just Collect Data. *The New York Times*, Available from:

http://www.nytimes.com/2015/04/19/technology/technology-that-prods-you-to-take-action-not-just-collect-data.html (accessed 1 April 2016).
Spencer Jr. BF, Ruiz-Sandoval ME and Kurata N (2004) Smart sensing technology: opportunities and challenges. *Structural Control and Health Monitoring*, 11(4), 349–368, Available from: http://doi.wiley.com/10.1002/stc.48.
Sterling B (2013) The Internet of Things: Quantified Self, IoT, Smart Cities, Smart Cars, Smart Clothes. *Wired*, Available from: http://www.wired.com/2013/04/the-internet-of-things-quantified-self-iot-smart-cities-smart-cars-smart-clothes/ (accessed 29 March 2016).
Stiegler B (n.d.) Anamnesis and Hypomnesis: Plato as the first thinker of the proletarianisation. *Ars Industrialis*, Available from: http://arsindustrialis.org/anamnesis-and-hypomnesis (accessed 1 April 2016).
Stinson L (2015) Having a Hard Time Being a Human? This App Manages Friendships for You. *Wired*, Available from: http://www.wired.com/2015/01/hard-time-human-app-manages-friendships/ (accessed 2 April 2016).
Swan M (2012) Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, 1(3), 217–253.
Swan M (2013) The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. *Big Data*, 1(2), 85–99.
The Decades That Invented the Future, Part 12: The Present and Beyond (2013) *Wired*, Available from: http://www.wired.com/2013/02/the-decades-that-invented-the-future-part-12-the-present-and-beyond/ (accessed 28 March 2016).
The 'Only' Coke Machine on the Internet (n.d.) *Carnegie Mellon University*, Available from: https://www.cs.cmu.edu/~coke/history_long.txt (accessed 28 March 2016).
Thrift N (2011) Lifeworld Inc—and what to do about it. *Environment and Planning D: Society and Space*, 29(1), 5–26.
Thync (n.d.) *Thync*, Available from: www.thync.com (accessed 28 March 2016).
Turner F (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, University of Chicago Press.
Turow J (2011) *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*. New Haven, Yale University Press.
Urist J (2015) From Paint to Pixels. *The Atlantic*, Available from: http://www.theatlantic.com/entertainment/archive/2015/05/the-rise-of-the-data-artist/392399/ (accessed 29 March 2016).
van Dijck J (2013) *The Culture of Connectivity: A Critical History of Social Media*. Cambridge, Oxford University Press.
Velasco JR (2016) Freeing Oneself from Power. *13/13: Michel Foucault's College de France Lectures*, Available from: http://blogs.law.columbia.edu/foucault1313/2016/02/09/freeing-oneself-from-power-on-the-government-of-the-living/ (accessed 29 March 2016).
Wadhwa V (2013) Five innovation predictions for 2013. *The Washington Post*, Available from: https://www.washingtonpost.com/national/on-innovations/five-

innovation-predictions-for-2013/2013/01/04/f4718be6-55c5-11e2-bf3e-76c0a789346f_story.html (accessed 28 March 2016).
Wajcman J and Rose E (2011) Constant Connectivity: Rethinking Interruptions at Work. *Organization Studies*, 32(7), 941–961.
Walker R (2010) Wasted Data. *New York Times*, Available from: http://www.nytimes.com/2010/12/05/magazine/05FOB-Consumed-t.html?mtrref=undefined&gwh=224196DF50B6FEC7F871890CABC54F5A&gwt=pay (accessed 29 March 2016).
Wallace L (2010) The Illusion of Control. *The Atlantic*, Available from: http://www.theatlantic.com/technology/archive/2010/05/the-illusion-of-control/57294/ (accessed 1 April 2016).
Wang X (2004) Smart Sensor and Smart Sensor Networks. *Proceedings of the 5th World Congress on Intelligent Control*, 3600–3606.
Watson SM (2013a) Living with Data: Personal Data Uses of the Quantified Self. University of Oxford.
Watson SM (2013b) The Latest Smartphones Could Turn Us All Into Activity Trackers. *Wired*, Available from: http://www.wired.com/2013/10/the-trojan-horse-of-the-latest-iphone-with-the-m7-coprocessor-we-all-become-qs-activity-trackers/ (accessed 29 March 2016).
Wearables Market to Be Worth $25 Billion by 2019 (2015) *CCS Insight*, Available from: http://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight (accessed 28 March 2016).
Weintraub K (2013) Quantified self: The tech based route to a better life? *BBC Future*, Available from: http://www.bbc.com/future/story/20130102-self-track-route-to-a-better-life (accessed 29 March 2016).
Wilson JH (2012) The Social Side of Auto-Analytics. *Harvard Business Review*, Available from: https://hbr.org/2012/09/the-social-side-of-auto-analytics.html (accessed 31 March 2016).
Wingfield N (2013) Gauging the Natural, and Digital, Rhythms of Life. *New York Times*, Available from: http://bits.blogs.nytimes.com/2013/06/19/gauging-the-natural-and-digital-rhythms-of-life/?_r=0 (accessed 28 March 2016).
Wolf G (2008) Reality Mining at MIT. *Quantified Self*, Available from: http://quantifiedself.com/2008/03/reality-mining-at-mit/ (accessed 29 March 2016).
Wolf G (2009a) Know Thyself: Tracking Every Facet of Life, from Sleep to Mood to Pain, 24/7/365. *Wired*, Available from: http://www.wired.com/2009/06/lbnp-knowthyself/ (accessed 1 April 2016).
Wolf G (2009b) The power of false remembering. *Quantified Self*, Available from: http://quantifiedself.com/2009/04/the-power-of-false-remembering/ (accessed 29 March 2006).
Wolf G (2010a) The Data-Driven Life. *New York Times*, Available from: http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?_r=1 (accessed 11 January 2014).
Wolf G (2010b) Tim Ferriss Wants to Hack Your Body. *Wired*, Available from: http://www.wired.com/2010/11/mf_qa_ferriss/ (accessed 29 March 2016).

Wolf G (2011) What is the Quantified Self? *Quantified Self*, Available from: http://quantifiedself.com/2011/03/what-is-the-quantified-self/ (accessed 30 March 2016).
Wolf G and Kelly K (2012) Wired's Gary Wolf & Kevin Kelly Talk the Quantified Self. In: *WIRED Health Conference: Living by Numbers*, New York, Available from: http://library.fora.tv/2012/10/15/Wireds_Gary_Wolf__Kevin_Kelly_Talk_the_Quantified_Self.
Wollman D (2014) Basis Peak review: a good fitness tracker, with room to be a good smartwatch. *Engadget*, Available from: http://www.engadget.com/2014/11/14/basis-peak-review/ (accessed 31 March 2016).
Worldwide Wearables Market Soars in the Third Quarter as Chinese Vendors Challenge the Market Leaders, According to IDC (2015) *International Data Corporation*, Available from: http://www.idc.com/getdoc.jsp?containerId=prUS40674715 (accessed 28 March 2016).
Zemrani L (2015) Using Self Tracking to Exercise More Efficiently. In: *New York Quantified Self Meetup*, New York.
Zimmer M (2008) The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0. *First Monday*, 13(3).
Zimmerman J (2014) There's a fitness tracker for vaginas. Quantifying your life has gone too far. *The Guardian*, Available from: http://www.theguardian.com/commentisfree/2014/jul/14/fitness-tracker-vagina-quantified-life (accessed 1 April 2016).
Žižek S (n.d.) The Interpassive Subject. Available from: http://www.egs.edu/faculty/slavoj-zizek/articles/the-interpassive-subject/.
Zuckerman E (2011) Kevin Kelly on context for the quantified self. *... My heart's in Accra*, Available from: http://www.ethanzuckerman.com/blog/2011/05/29/kevin-kelly-on-context-for-the-quantified-self/ (accessed 2 April 2016).

CHAPTER THREE

A Strategy for Surveillance Powers (2013) *The New York Times*, Available from: http://www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html (accessed 27 March 2016).
Aaronson T (2013) *The Terror Factory: Inside the FBI's Manufactured War on Terrorism*. Brooklyn: IG Publishing.
Aaronson T (2015) The Sting: How the FBI Created a Terrorist. *The Intercept*, Available from: https://theintercept.com/2015/03/16/howthefbicreatedaterrorist/ (accessed 19 March 2016).

Adey P (2009) Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space*, 27(2), 274–295.
Adey P and Anderson B (2012) Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue*, 43(2), 99–117.
American Civil Liberties Union v. National Security Agency 493 F.3d 644 (E.D. Mich., 2007), Available from: https://www.aclu.org/files/pdfs/safefree/nsamemo.opinion.judge.taylor.081706.pdf
Ananny M (2016) Toward an Ethics of Algorithms: Convening, Observation, Probability, and Timeliness. *Science, Technology & Human Values*, 41(1), 93–117, Available from: http://sth.sagepub.com/cgi/doi/10.1177/0162243915606523.
Andrejevic M (2005) The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479–497.
Andrejevic M (2010) Surveillance and Alienation in the Online Economy. *Surveillance & Society*, 8(3), 278–287.
Andrejevic M (2013) *InfoGlut: How Too Much Information Is Changing the Way We Think and Know*. New York, Routledge.
Angwin J (2014) *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York, Times Books.
Anthony S (2015) Pre-crime arrives in the UK with a crowdsourced watch list. *Ars Technica*, Available from: http://arstechnica.com/tech-policy/2015/12/pre-crime-arrives-in-the-uk-better-make-sure-your-face-stays-off-the-crowdsourced-watch-list/ (accessed 18 March 2016).
AP's Probe Into NYPD Intelligence Operations (2012) *Associated Press*, Available from: http://www.ap.org/Index/AP-In-The-News/NYPD (accessed 18 March 2016).
Aradau C and van Munster R (2007) Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. *European Journal of International Relations*, 13(1), 89–115.
Aradau C and van Munster R (2011) *The Politics of Catastrophe: Genealogies of the Unknown*. London, Routledge.
Aradau C and van Munster R (2012) The Time/Space of Preparedness: Anticipating the 'Next Terrorist Attack'. *Space and Culture*, 15(2), 98–109.
Asaro PM (2013) The labor of surveillance and bureaucratized killing: new subjectivities of military drone operators. *Social Semiotics*, 23(2), 196–224.
Bamford J (2008) *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York, Doubleday.
Barker G (2016) Homegrown: The Counter-Terror Dilemma. USA, Available from: http://www.hbo.com/documentaries/homegrown-the-counter-terror-dilemma.
Barrett R (2013) Don't turn security into theater. *CNN*, Available from: http://globalpublicsquare.blogs.cnn.com/2013/05/06/dont-turn-security-into-theater/ (accessed 9 March 2016).
Bauman Z and Lyon D (2013) *Liquid Surveillance: A Conversation*. Cambridge, Polity.
Beck U (1992) *Risk Society: Towards a New Modernity*. London, SAGE.

Beck U (2002) The Terrorist Threat: World Risk Society Revisited. *Theory, Culture & Society*, 19(4), 39–55.
Beck U (2009) *World at Risk*. Malden, Polity Press.
Becker J and Shane S (2012) Secret 'Kill List' Proves a Test of Obama's Principles and Will. *The New York Times*, Available from: http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?pagewanted=1&_r=1 (accessed 20 March 2016).
Bergen PL (2016) *United States of Jihad - Investigating America's Homegrown Terrorists*. New York: Crown Publishers.
Blair T (2004) Full text: Tony Blair's speech. *The Guardian*, Available from: http://www.theguardian.com/politics/2004/mar/05/iraq.iraq (accessed 26 March 2016).
Bohan C (2013) Lawmakers urge review of domestic spying, Patriot Act. *Chicago Tribune*, Available from: http://articles.chicagotribune.com/2013-06-09/news/sns-rt-us-usa-security-lawmakersbre9580ab-20130609_1_guardian-national-security-agency-surveillance (accessed 26 March 2016).
Bump P (2013) You'll Never Know if the NSA Is Breaking the Law — or Keeping You Safe. *The Atlantic*, Available from: http://www.thewire.com/politics/2013/06/nsa-surveillance-legal/66681/ (accessed 30 January 2015).
Burris S (2016) 'Minority Report' is coming true: We now have threat scores to match our credit scores. *Salon*, Available from: http://www.salon.com/2016/01/15/minority_report_is_coming_true_we_now_have_threat_scores_to_match_our_credit_scores_partner/ (accessed 18 March 2016).
Calamur K (2016) NYPD Settles Pair of Lawsuits Over Muslim Surveillance. *The Atlantic*, Available from: http://www.theatlantic.com/national/archive/2016/01/nypd-surveillance-muslims-settlement/423174/ (accessed 18 March 2016).
Clarke RA, Morell MJ, Stone GR, et al. (2013) *Liberty and Security in a Changing World*. Available from: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
Cohen JE (2013) What Privacy Is For. *Harvard Law Review*, 126, 1904–1933.
Coleman G (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, Verso.
Cooper M (2006) Pre-empting Emergence: The Biological Turn in the War on Terror. *Theory, Culture & Society*, 23(4), 113–135.
Crary J (2013) *24/7: Late Capitalism and the Ends of Sleep*. London, Verso.
Daase C and Kessler O (2007) Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger. *Security Dialogue*, 38(4), 411–434.
Davidson A (2015) Unclear Dangers. *New Yorker*, Available from: http://www.newyorker.com/magazine/2015/05/18/unclear-dangers (accessed 19 March 2016).
Dean M (1998) Risk, Calculable and Incalculable. *Soziale Welt*, 49, 25–42.

Debord G (1990) *Comments on the Society of the Spectacle*. London: Verso.
Delany SR (1971) About Five Thousand One Hundred and Seventy Five Words. In: Clareson TD (ed.), *Sf: The Other Side of Realism*, Bowling Green, Bowling Green University Popular Press, pp. 130–146.
Devereaux R (2015) Manhunting in the Hindu Kush. *The Intercept*, Available from: https://theintercept.com/drone-papers/manhunting-in-the-hindu-kush/ (accessed 20 March 2016).
Doctorow C (2016) Exclusive: Snowden intelligence docs reveal UK spooks' malware checklist. *Boingboing*, Available from: http://boingboing.net/2016/02/02/doxxing-sherlock-3.html (accessed 27 March 2016).
Douglas M (2001) Dealing with uncertainty. *Ethical Perspectives*, 8(3), 145–155.
Edward Snowden SXSW: Full Transcript and Video (2014) *Inside.com*, Available from: http://blog.inside.com/blog/2014/3/10/edward-snowden-sxsw-full-transcription-and-video (accessed 19 March 2014).
Eliasoph N (1998) *Avoiding politics: How Americans produce apathy in everyday*. Cambridge, Cambridge University Press.
Elliott J and Meyer T (2013) Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence. *ProPublica*, Available from: http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence (accessed 21 March 2016).
Ewald F (1993) Two Infinities of Risk. In: Massumi B (ed.), *The Politics of Everyday Fear*, Minneapolis, University of Minnesota Press, pp. 221–228.
Fallows J (n.d.) James Fallows. *The Atlantic*, Available from: http://www.theatlantic.com/author/james-fallows/?page=2 (accessed 26 March 2016).
Foucault M (1998) *The Will to Knowledge*. London, Penguin Books.
Fressoz J-B (2007) Beck Back in the 19th Century: Towards a Genealogy of Risk Society. *History and Technology*, 23(4), 333–350.
Friedersdorf C (2013) The Surveillance State Puts U.S. Elections at Risk of Manipulation. *The Atlantic*, Available from: http://www.theatlantic.com/politics/archive/2013/11/the-surveillance-state-puts-us-elections-at-risk-of-manipulation/281232/ (accessed 18 March 2016).
Friedersdorf C (2014) New Surveillance Whistleblower: The NSA Violates the Constitution. *The Atlantic*, Available from: http://www.theatlantic.com/politics/archive/2014/07/a-new-surveillance-whistleblower-emerges/374722/ (accessed 21 March 2016).
Funtowicz SO and Ravetz JR (1993) The Emergence of Post-Normal Science. In: von Schomberg R (ed.), *Science, Politics and Morality: Scientific Uncertainty and Decision Making*, Springer-Science+Business Media, B.V., pp. 85–123.
Gan V (2013) How TV's 'Person of Interest' Helps Us Understand the Surveillance Society. *Smithsonian.com*, Available from: http://www.smithsonianmag.com/smithsonian-institution/how-tvs-person-of-interest-helps-us-understand-the-surveillance-society-5407171/?no-ist (accessed 24 October 2013).

Gates KA (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York, New York University Press.
Gerbner G, Gross L and Morgan M (1980) The 'Mainstreaming' of America: Violence Profile No. 11. *Journal of Communication*, 30(3), 10–29.
Gerstein J (2007) Spies Prep Reporters on Protecting Secrets. *New York Sun*, Available from: http://www.nysun.com/national/spies-prep-reporters-on-protecting-secrets/63465/ (accessed 21 March 2016).
Giddens A (1990) *The Consequences of Modernity*. Cambridge, Polity Press.
Goldberg J (2016) The Obama Doctrine. *The Atlantic*, Available from: http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/#article-comments (accessed 10 March 2016).
Gould SJ (1996) *The Mismeasure of Man: The definitive refutation to the argument of The Bell Curve*. New York, W.W. Norton & Co.
Greenberg A (2014) How to Anonymize Everything You Do Online. *Wired*, Available from: http://www.wired.com/2014/06/be-anonymous-online/ (accessed 18 March 2016).
Greenwald G (2014a) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London, Penguin Books.
Greenwald G (2014b) Why privacy matters. *TED*, Available from: http://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript (accessed 26 March 2016).
Greenwald G (2016) Nobody Knows the Identities of the 150 People Killed by U.S. in Somalia, but Most Are Certain They Deserved It. *The Intercept*, Available from: https://theintercept.com/2016/03/08/nobody-knows-the-identity-of-the-150-people-killed-by-u-s-in-somalia-but-most-are-certain-they-deserved-it/ (accessed 20 March 2016).
Gregory D (2011) From a View to a Kill: Drones and Late Modern War. *Theory, Culture & Society*, 28(7-8), 188–215.
Hacking I (1990) *The Taming of Chance*. Cambridge, Cambridge University Press.
Han B-C (2010) *Müdigkeitsgesellschaft*. Berlin, Matthes & Seitz.
Hannah MG (2010) (Mis)adventures in Rumsfeld Space. *GeoJournal*, 75(4), 397–406.
Hayden M (2002) Statement for the Record. *Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committe on Intelligence.* Hearing.
Hayden M (2006) Remarks by General Michael V. Hayden. In: *National Press Club*, Washington D.C.
Hayden M (2016) *Playing To The Edge: American Intelligence in the Age of Terror*. New York, Penguin Press.
Hearings *Senate Intelligence Committee*, Available from: http://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-against-united-states# (accessed 21 March 2016).
Hendrix J (2013) NSA surveillance puts George Orwell's '1984' on bestseller lists. *Los Angeles Times*, Available from: http://articles.latimes.com/2013/jun/11/entertainment/la-et-jc-nsa-surveillance-puts-george-orwells-1984-on-bestseller-lists-20130611 (accessed 11 March 2014).

Hong S (2014) The other-publics: Mediated othering and the public sphere in the Dreyfus Affair. *European Journal of Cultural Studies*, 17(6), 665–681.
Horn E (2012) Logics of Political Secrecy. *Theory, Culture & Society*, 28(7-8), 103–122.
Hu T-H (2015) *The Prehistory of the Cloud*. Cambridge, MIT Press.
HUMINT May Be Getting Harder to Do, But SIGINT Continues to Rise in Importance (2015) *The Economist*. Print Edition.
Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions (2014) Available from: https://www.hrw.org/sites/default/files/reports/usterrorism0714_ForUpload_1_0.pdf.
Kirn W (2015) If You're Not Paranoid, You're Crazy. *The Atlantic*, Available from: http://www.theatlantic.com/magazine/archive/2015/11/if-youre-not-paranoid-youre-crazy/407833/ (accessed 18 March 2016).
Knappenberger B (2013) Why Care About the N.S.A.? *New York Times*, Available from: http://www.nytimes.com/video/opinion/100000002571435/why-care-about-the-nsa.html (accessed 11 February 2014).
Knowlton B (2013) Feinstein 'Open' to Hearings on Surveillance Programs. *New York Times*, Available from: http://thecaucus.blogs.nytimes.com/2013/06/09/lawmaker-calls-for-renewed-debate-over-patriot-act/?_php=true&_type=blogs&_r=0.
Kozaryn LD (2002) Alleged Al Qaeda 'Dirty Bomb' Operative in U.S. Military Custody. *US Department of Defense*, Available from: http://archive.defense.gov/news/newsarticle.aspx?id=43767 (accessed 19 March 2016).
Lake E (2014) Spy Chief: We Should've Told You We Track Your Calls. *The Daily Beast*, Available from: http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html.
Laprise J (2016) Exploring PRISM's Spectrum: Privacy in the Information Age. In: Musiani F, Cogburn DL, DeNardis L, et al. (eds), *The Turn to Infrastructure in Internet Governance*, Basingstoke, Palgrave Macmillan.
Laskow S (2013) A new film shows how much we knew, pre-Snowden, about Internet surveillance. *Columbia Journalism Review*, Available from: http://www.cjr.org/cloud_control/a_new_film_shows_exactly_how_m.php.
Latour B (2013) *An Inquiry into Modes of Existence: An Anthropology of the Moderns*. Cambridge, Harvard University Press.
Lears J (2003) *Something for Nothing: Luck in America*. New York, Viking.
Ledgett R (2014) The NSA responds to Edward Snowden's TED Talk. *TED 2014*, Available from: http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk.
Lee M (2015) Edward Snowden Explains How To Reclaim Your Privacy. *The Intercept*, Available from: https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/ (accessed 18 March 2016).
Leonnig C (2013) Court: Ability to police U.S. spying program limited. *The Washington Post*, Available from: http://www.washingtonpost.com/politics/court-

ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html (accessed 1 February 2015).
Lepore J (2016) After the Fact. *New Yorker*, Available from: http://www.newyorker.com/magazine/2016/03/21/the-internet-of-us-and-the-end-of-facts?mbid=social_facebook (accessed 26 March 2016).
Lovece F (2014) Soldier showdown: Joe and Anthony Russo take the helm of 'Captain America' franchise. *Filmjournal*, Available from: http://www.filmjournal.com/node/9232 (accessed 26 March 2016).
Margolis G (2013) The Lack of HUMINT: A Recurring Intelligence Problem. *Global Security Studies*, 4(2), 43–60.
Marlinspike M (2013) Why 'I Have Nothing to Hide' Is the Wrong Way to Think About Surveillance. *Wired*, Available from: http://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/ (accessed 26 March 2016).
Martin R (2002) *The Financialization of Daily Life*. Philadelphia, Temple University Press.
Massumi B (2005) Fear (The spectrum said). *positions*, 13(1), 31–48.
Massumi B (2007) Potential Politics and the Primacy of Preemption. *Theory & Event*, 10(2).
Massumi B (2010) The Future Birth of the Affective Fact: The Political Ontology of Threat. In: Gregg M and Seigworth GJ (eds), *The Affect Theory Reader*, Durham, Duke University Press, pp. 52–70.
Matviyenko S (2015) Interpassive User: Complicity and the Returns of Cybernetics. *The Fibreculture Journal*, The Fibreculture Journal, (25), 135–163, Available from: http://twentyfive.fibreculturejournal.org/fcj-184-interpassive-user-complicity-and-the-returns-of-cybernetics/.
Milburne C (2015) {Zero Day} // Hacking as Applied Science Fiction. In: *Department of History and Sociology of Science Fall 2015 Monday Workshop series*, University of Pennsylvania, Philadelphia.
Milner M (2013) Did Edward Snowden tell us anything we didn't already know? *Chicago Reader*, Available from: http://www.chicagoreader.com/Bleader/archives/2013/06/25/did-edward-snowden-tell-us-anything-we-didnt-already-know.
Moeckli D (2008) *Human Rights and Non-discrimination in the 'War on Terror'*. Oxford, Oxford University Press.
Molotch HL (2012) *Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger*. Princeton, Princeton University Press.
Monahan T (2010) *Surveillance in the Time of Insecurity*. New Brunswick, Rutgers University Press.
Monahan T (2015) The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies*, 12(2), 159–178.
Moon IC and Carley KM (2007) Modeling and simulating terrorist networks in social and geospatial dimensions. *IEEE Intelligent Systems*, 22(5), 40–49.

Nakashima E (2013) NSA cites case as success of phone data-collection program. *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html (accessed 19 March 2016).

NSA Chief Keith Alexander Keynote @ Black Hat USA 2013 (w/ Slide Presentation) (2013) *Leaksource*, Available from: http://leaksource.info/2013/08/01/nsa-chief-keith-alexander-keynote-black-hat-usa-2013-w-slide-presentation/ (accessed 21 March 2016).

O'Harrow Jr R (2013) NSA chief asks a skeptical crowd of hackers to help agency do its job. *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/nsa-chief-asks-a-skeptical-crowd-of-hackers-to-help-agency-do-its-job/2013/07/31/351096e4-fa15-11e2-8752-b41d7ed1f685_story.html (accessed 21 March 2016).

O'Malley P (2004) *Risk, Uncertainty and Government*. London, Glasshouse Press.

Obama B (2013) Transcript: Obama's Remarks on NSA Controversy. *The Wall Street Journal*, Available from: http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/.

Operations Security (OPSEC) (n.d.) *US Department of Defense Education Activity*, Available from: http://www.dodea.edu/offices/safety/opsec.cfm (accessed 18 March 2016).

Packer G (2014) The Holder of Secrets. *The New Yorker*, Available from: http://www.newyorker.com/magazine/2014/10/20/holder-secrets (accessed 26 March 2016).

Patterson J (2013) How Hollywood softened us up for NSA surveillance. *The Guardian*, Available from: http://www.theguardian.com/film/shortcuts/2013/jun/16/hollywood-softened-us-up-nsa-surveillance (accessed 26 March 2016).

Pfaller R (2001) Interpassivity and Misdemeanors. The Analysis of Ideology and the Zizekian Toolbox. *International Journal of Zizek Studies*, 1(1), 33–50.

Pfaller R (2003) Little Gestures of Disappearance(1) Interpassivity and the Theory of Ritual. *Journal of European Psychoanalysis*, 16.

Powell C (2003) Full text of Colin Powell's speech. *The Guardian*, Available from: http://www.theguardian.com/world/2003/feb/05/iraq.usa (accessed 20 March 2016).

Rappaport R (1999) *Ritual and Religion in the Making of Humanity*. Cambridge, Cambridge University Press.

Risen J and Poitras L (2013) N.S.A. Report Outlined Goals for More Power. *New York Times*, Available from: http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html (accessed 26 March 2016).

Romer D and Jamieson P (2014) Violence in Popular U.S. Prime Time TV Dramas and the Cultivation of Fear: A Time Series Analysis. *Media and Communication*, 2(2), Available from: http://www.cogitatiopress.com/ojs/index.php/mediaandcommunication/article/view/8.

Rothman J (2014) 'Person of Interest': The TV Show That Predicted Edward Snowden. *The New Yorker*, Available from: http://www.newyorker.com/culture/culture-desk/person-of-interest-the-tv-show-that-predicted-edward-snowden (accessed 26 March 2016).

Rowan D (2014) Snowden: Big revelations to come, reporting them is not a crime. *Wired.co.uk*, Available from: http://www.wired.co.uk/news/archive/2014-03/18/snowden-ted.

Rusbridger A, Gibson J and MacAskill E (2015) Edward Snowden: NSA reform in the US is only the beginning. *The Guardian*, Available from: http://www.theguardian.com/us-news/2015/may/22/edward-snowden-nsa-reform (accessed 26 March 2016).

Schneier B (2013) It's smart politics to exaggerate terrorist threats. *CNN*, Available from: http://www.cnn.com/2013/05/20/opinion/schneier-security-politics/ (accessed 10 March 2016).

Scholzel H (2014) Beyond Interactivity. The Interpassive Hypotheses on 'Good Life ' and Communication. In: *ICA 2014*, Seattle.

Schüll ND (2014) *Addiction by Design: Machine Gambling in Las Vegas*. Princeton, Princeton University Press.

Schwartz M (2015) The Whole Haystack. *The New Yorker*, Available from: http://www.newyorker.com/magazine/2015/01/26/whole-haystack (accessed 15 February 2015).

Sekula A (1986) The Body and the Archive. *October*, 39, 3–64.

Selvaggio L (n.d.) URME Surveillance. Available from: http://www.urmesurveillance.com/ (accessed 18 March 2016).

Shaver A (2015) You're more likely to be fatally crushed by furniture than killed by a terrorist. *The Washington Post*, Available from: https://www.washingtonpost.com/news/monkey-cage/wp/2015/11/23/youre-more-likely-to-be-fatally-crushed-by-furniture-than-killed-by-a-terrorist/ (accessed 9 March 2016).

Sifton J (2012) A Brief History of Drones. *The Nation*, Available from: http://www.thenation.com/article/brief-history-drones/ (accessed 20 March 2016).

Silverstein K (2015) US Reliance on Too Much SIGINT and Too Little Spycraft Is Dangerous and Expensive. *Observer*, Available from: http://observer.com/2015/09/us-reliance-on-too-much-sigint-and-too-little-spycraft-is-dangerous-and-expensive/ (accessed 26 March 2016).

Singer PW (2009a) Military robots and the future of war. *The New Atlantis*, 23, 25–45.

Singer PW (2009b) *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York, Penguin.

Sloterdijk P (1987) *Critique of Cynical Reason*. Minneapolis, University of Minnesota Press.

Snowden E (2013) Whistleblower Edward Snowden gives 2013's Alternative Christmas Message. *Channel4.com*, Available from: http://www.channel4.com/programmes/alternative-christmas-message/on-demand/58816-001 (accessed 22 February 2014).

Snowden E (2016) No Title. *Twitter*, Available from: https://twitter.com/snowden/status/711567142865522690 (accessed 27 March 2016).
Sterman D (2014) Infographic: How the Government Exaggerated the Successes of NSA Surveillance. *Slate*, Available from: http://www.slate.com/blogs/future_tense/2014/01/16/nsa_surveillance_how_the_government_exaggerated_the_way_its_programs_stopped.html (accessed 21 March 2016).
Surveillance Camera Man (n.d.) Available from: https://www.youtube.com/user/SurveillantCameraMan (accessed 18 March 2016).
Taussig M (1999) *Defacement - Public Secrecy and the Labour of the Negative*. Stanford, Stanford University Press.
Taylor E (2013) *Surveillance Schools: Security, Discipline and Control in Contemporary Education*. Basingstoke, Palgrave Macmillan.
Terranova T (2000) Free Labor: Producing Culture for the Digital Economy. *Social Text*, 18(2), 33–58.
Transcript: Senate Intelligence hearing on national security threats (2014) *The Washington Post*, Available from: https://www.washingtonpost.com/world/national-security/transcript-senate-intelligence-hearing-on-national-security-threats/2014/01/29/b5913184-8912-11e3-833c-33098f9e5267_story.html (accessed 21 March 2016).
Turner V (1982) Liminal to Liminoid. In: Turner V (ed.), *Play, Flow, Ritual: An Essay in Comparative Symbology*, New York, Performing Arts Journal Publishing, pp. 53–92.
Van Buren P (2013) 10 Myths About NSA Surveillance That Need Debunking. *MotherJones*, Available from: http://www.motherjones.com/politics/2014/01/10-myths-nsa-surveillance-debunk-edward-snowden-spying (accessed 13 January 2014).
van Oenen G (2002) Interpassivity revisited: a critical and historical reappraisal of interpassive phenomena. *International Journal of Zizek Studies*, 2(2).
van Oenen G (2006) A Machine That Would Go of Itself: Interpassivity and Its Impact on Political Life. *Theory & Event*, 9(2).
Vickers D and Leno J (2013) The Tonight Show with Jay Leno. USA, NBC, Available from: https://www.youtube.com/watch?v=jOW0Z2Czgzk.
Walker Leads Tightly Clustered GOP Field, Clinton Up Big Nationally (2015) *Public Policy Polling*, Available from: http://www.publicpolicypolling.com/pdf/2015/PPP_Release_National_51315.pdf (accessed 19 March 2016).
We Already Knew The NSA Spies On Us. We Already Know Everything. Everything Is Boring. (2015) *Clickhole*, Available from: http://www.clickhole.com/article/we-already-knew-nsa-spies-us-we-already-know-every-1876.
Woods C (2015) The Story of America's Very First Drone Strike. *The Atlantic*, Available from: http://www.theatlantic.com/international/archive/2015/05/america-first-drone-strike-afghanistan/394463/ (accessed 20 March 2016).

Yaverbaum E (2014) The War on Privacy Is Over. *The Huffington Post*, Available from: http://www.huffingtonpost.com/eric-yaverbaum/the-war-on-privacy-is-ove_b_4949429.html.
Žižek S (1998) The inherent transgression. *Cultural Values*, 2(1), 1–17, Available from: http://www.tandfonline.com/doi/abs/10.1080/14797589809359285 (accessed 2 March 2015).
Žižek S (n.d.) The Interpassive Subject. Available from: http://www.egs.edu/faculty/slavoj-zizek/articles/the-interpassive-subject/.

CHAPTER FOUR

Allen A (2014) Feeling mad? New devices can sense your mood and tell — or even text — others. *The Washington Post*, Available from: https://www.washingtonpost.com/national/health-science/feeling-mad-new-devices-can-sense-your-mood-and-tell--or-even-text--others/2014/01/13/8436009c-6275-11e3-91b3-f2bb96304e34_story.html (accessed 13 April 2016).
Barol B (2015) This Sleek Sleep-Sensing Orb Promises A Good Night's Rest. *Fast Company*, Available from: http://www.fastcompany.com/3042760/sleep-week/this-sleek-sleep-sensing-orb-promises-a-good-nights-rest (accessed 4 May 2016).
Bauman Z and Lyon D (2013) *Liquid Surveillance: A Conversation*. Cambridge, Polity.
Benvie D (2013) The commercial benefits of the Quantified Self. *PR Week*, Available from: http://www.prweek.com/article/1215077/commercial-benefits-quantified-self (accessed 5 May 2016).
Bowden M (2012) The Measured Man. *The Atlantic*, Available from: http://www.theatlantic.com/magazine/archive/2012/07/the-measured-man/309018/ (accessed 11 July 2015).
Boyd D and Crawford K (2012) Critical Questions for Big Data. *Information, Communication & Society*, 15(5), 662–679.
Bratich J (2006) Public Secrecy and Immanent Security. *Cultural Studies*, 20(4-5), 493–511.
Brennan S (2015) Awareables: The Technology of Superhumans. *Wired*, Available from: http://www.wired.com/insights/2015/03/awareables-technology-superhumanism/ (accessed 13 April 2016).
Cha AE (2015) The revolution will be digitized. *The Washington Post*, Available from: http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/ (accessed 13 April 2016).
Chandler JA (2012) 'Obligatory Technologies': Explaining Why People Feel Compelled to Use Certain Technologies. *Bulletin of Science, Technology & Society*, 32(4), 255–264.
Cheney-Lippold J (2011) A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, 28(6), 164–181.

Chun WHK (2006) *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge, MIT Press.

Cohen J (2012) The Patient of the Future. *MIT Technology Review*, Available from: https://www.technologyreview.com/s/426968/the-patient-of-the-future/ (accessed 13 April 2016).

Cornell M (2011) The Big Bucket Personal Informatics Data Model. *Quantified Self*, Available from: http://quantifiedself.com/2011/02/the-big-bucket-personal-informatics-data-model/ (accessed 13 April 2016).

Crawford K, Lingel J and Karppi T (2015) Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies*, 18(4-5), 479–496.

Dancy C (2015) Mindful Devices: Nonjudgmental Living in a Connected World. In: *Quantified Self 2015 Conference*, San Francisco.

Daston LJ (1992) Objectivity and the Escape from Perspective. *Social Studies of Science*, 22, 597–618.

Daston LJ and Galison P (2007) *Objectivity*. New York, Zone Books.

Dembosky A (2011) Invasion of the body hackers. *Financial Times*, Available from: https://next.ft.com/content/3ccb11a0-923b-11e0-9e00-00144feab49a (accessed 14 April 2016).

Eamon W (1994) *Science and the Secrets of Nature: Books of Secrets in Medieval and Early Modern Culture*. Princeton, Princeton University Press.

Edgerton D (2010) Innovation, Technology, or History: What is the Historiography of Technology About? *Technology and Culture*, 51(3), 680–697.

Eisen J (2015) What does the term microbiome mean? And where did it come from? A bit of a surprise .. *Microbenet*, Available from: http://microbe.net/2015/04/08/what-does-the-term-microbiome-mean-and-where-did-it-come-from-a-bit-of-a-surprise/ (accessed 5 May 2016).

Ellul J (1964) *The Technological Society*. New York, Knopf.

Fawcett T (2016) Mining the Quantified Self: Personal Knowledge Discovery as a Challenge for Data Science. *Big Data*, 3(4), 249–266.

Finley K (2013) Interview: Sensor Hacking For Mindfulness with Nancy Dougherty on the new Mindful Cyborgs. *Technoccult*, Available from: http://technoccult.net/archives/2013/06/10/interview-sensor-hacking-for-mindfulness-with-nancy-dougherty-on-the-new-mindful-cyborgs/ (accessed 11 April 2015).

Fleck L (1979) *Genesis and Development of a Scientific Fact*. Trenn TJ and Merton RK (eds), Chicago, University of Chicago Press.

Flichy P (2007) *The Internet Imaginaire*. Cambridge, MIT Press.

Fotopoulou A and O'Riordan K (2015) Biosensory experiences and media materiality Fitbit and biosensors: imaginaries and material instantiations. In: *IR16*, Phoenix, Arizona.

Freund PES (2004) Civilised Bodies Redux: Seams in the Cyborg. *Social Theory & Health*, 2(3), 273–289.

Garten A (2011) Know thyself, with a brain scanner. *TED*, Available from: https://www.ted.com/talks/ariel_garten_know_thyself_with_a_brain_scanner/transcript?language=en (accessed 22 June 2012).
Gillespie T (2010) The politics of 'platforms'. *New Media & Society*, 12(3), 347–364.
Goetz T (2011) Harnessing the Power of Feedback Loops. *Wired*, Available from: http://www.wired.com/2011/06/ff_feedbackloop/2/ (accessed 13 April 2016).
Haggerty KD and Ericson R V (2000) The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622.
Hayles KN (1999) *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago, University of Chicago Press.
Hello (2014) Sense: Know More. Sleep Better. *Kickstarter*, Available from: https://www.kickstarter.com/projects/hello/sense-know-more-sleep-better/description (accessed 13 April 2016).
Hong S (2015) Presence: the sense of being-there and being-with in the new media society. *First Monday*, 20(10).
Hooper L V and Gordon JI (2001) Commensal Host-Bacterial Relationships in the Gut. *Science*, 292(5519), 1115–1118, Available from: http://science.sciencemag.org/content/292/5519/1115.
Houghton Jr. WE (1942) The English Virtuoso in the Seventeenth Century: Part I. *Journal of the History of Ideas*, 3(1), 51–73.
Hu T-H (2015) *The Prehistory of the Cloud*. Cambridge, MIT Press.
Hunter M (1989) *Establishing the New Science: The Experience of the Early Royal Society*. Woodbridge, Boydell Press.
Jain R and Jalali L (2014) Objective self. *IEEE Multimedia*, 21(4), 100–110.
Jordan M and Pfarr N (2014) Forget the Quantified Self. We Need to Build the Quantified Us. *Wired*, Available from: http://www.wired.com/2014/04/forget-the-quantified-self-we-need-to-build-the-quantified-us/ (accessed 29 March 2016).
Kelly K (2011) Self-Tracking? You Will. *KK*, Available from: http://kk.org/thetechnium/self-tracking-y/ (accessed 13 April 2016).
Kelly SM (2014) The Most Connected Man Is You, Just a Few Years From Now. *Mashable*, Available from: http://mashable.com/2014/08/21/most-connected-man/#I60SjAremkqw (accessed 14 April 2016).
Kline R (2001) Technological Determinism. In: *International Encyclopedia of the Social and Behavioral Sciences*, New York, Elsevier, pp. 15495–15498.
Kuhn TS (1962) *The Structure of Scientific Revolutions*. Chicago, University of Chicago Press, Available from: http://bibliovault.org/BV.landing.epl?ISBN=9780226458083.
Kvedar J (2011) A Physician's Perspective on Self-tracking. *MIT Technology Review*, Available from: https://www.technologyreview.com/s/424474/a-physicians-perspective-on-self-tracking/ (accessed 14 April 2016).
Lai M and Forzani E (2015) New Sensors, New Senses. In: *Quantified Self 2015 Conference*, San Francisco.
Lakoff G and Johnson M (1980) *Metaphors We Live By*. Chicago, University of Chicago Press.

Landes D (1969) *The Unbound Prometheus: Technological Change and Industrial Development in Western Europe from 1750 to the Present*. Cambridge, Cambridge University Press.

Lederberg J (2001) 'Ome Sweet 'Omics-- A Genealogical Treasury of Words. *The Scientist*, Available from: http://www.the-scientist.com/?articles.view/articleNo/13313/title/-Ome-Sweet--Omics---A-Genealogical-Treasury-of-Words/ (accessed 5 May 2016).

Lupton D (2013) Understanding the Human Machine. *IEEE Technology and Society Magazine*, 32(4), 25–30.

Lupton D (2014) Self-tracking cultures: towards a sociology of personal informatics. In: *OzCHI '14: Proceedings of the 26th Australian Computer-Human Interaction Conference: Designing Futures, the Future of Design*, Sydney.

Lupton D (2016) Self-tracking practices as knowledge technologies. *This Sociological Life*, Available from: https://simplysociology.wordpress.com/tag/self-tracking/ (accessed 13 April 2016).

MacLeod C (2007) *Heroes of Invention: Technology, Liberalism and British Identity, 1750-1914*. Cambridge, Cambridge University Press.

Manjoo F (2015) Mysteries of Sleep Lie Unsolved. *The New York Times*, Available from: http://www.nytimes.com/2015/02/26/technology/personaltech/despite-the-promise-of-technology-the-mysteries-of-sleep-lie-unsolved.html?_r=0 (accessed 4 May 2016).

Marvin C (1988) *When Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century*. Oxford, Oxford University Press.

Marx L (1994) The Idea of 'Technology' and Postmodern Pessimism. In: Smith MR and Marx L (eds), *Does Technology Drive History? The Dilemma of Technological Determinism*, Cambridge, MIT Press, pp. 237–258.

Marx L (2010) Technology: The Emergence of a Hazardous Concept. *Technology and Culture*, 51(3), 561–577.

Matyszczyk C (2012) How to work out if you are a datasexual. *Cnet*, Available from: http://www.cnet.com/news/how-to-work-out-if-you-are-a-datasexual/ (accessed 13 April 2016).

McLuhan M (1962) *The Gutenberg Galaxy: The Making of Typographic Man*. London, Routledge & Kegan Paul.

McLuhan M (1964) *Understanding Media: The Extensions of Man*. New York, Mentor.

Mearian L (2015) Insurance company now offers discounts - if you let it track your Fitbit. *Computerworld*, Available from: http://www.computerworld.com/article/2911594/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html (accessed 6 May 2016).

Meet Sense (n.d.) *Hello.is*, Available from: https://hello.is/videos#meet-sense (accessed 13 April 2016).

Merleau-Ponty M (1996) Eye and Mind. In: Johnson GA (ed.), *The Merleau-Ponty Aesthetics Reader*, Evanston, Northwestern University Press, pp. 121–149.

Merleau-Ponty M (2012) *Phenomenology of Perception*. London, Routledge.

Mortensen P (2013) The Future Of Technology Isn't Mobile, It's Contextual. *Fast Company*, Available from: http://www.fastcodesign.com/1672531/the-future-of-technology-isnt-mobile-its-contextual (accessed 13 April 2016).
Mumford L (1963) *Technics and Civilization*. New York, Harcourt, Brace and World.
Musson AE and Robinson E (1969) *Science and Technology in the Industrial Revolution*. Manchester, Manchester University Press.
No Title (n.d.) *Data Sense*, Available from: makesenseofdata.com (accessed 13 April 2016).
Nye DE (1994) *American Technological Sublime*. Cambidge, MIT Press.
Nyong'o T (2015) Plenary 4. In: *Affect Theory Conference | Worldings | Tensions | Futures*, Lancaster, PA.
Peters A (2013) This Scary Gadget Zaps You When You Get Lazy. *Fast Company*, Available from: http://www.fastcoexist.com/3023294/this-scary-gadget-zaps-you-when-you-get-lazy?partner=newsletter#6 (accessed 13 April 2016).
Peters JD (1999) *Speaking into the Air: A History of the Idea of Communication*. Chicago, University of Chicago Press.
Peters JD (2015) *The Marvelous Clouds: Toward a Philosophy of Elemental Media*. Chicago, University of Chicago Press.
Peysakhovich A and Stephens-Davidowitz S (2015) How Not to Drown in Numbers. *New York Times*, Available from: http://www.nytimes.com/2015/05/03/opinion/sunday/how-not-to-drown-in-numbers.html?_r=2 (accessed 13 April 2016).
Porter TM (1995) *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton, Princeton University Press.
Porter TM (2014) The Objective Self. *Victorian Studies*, 50(4), 641–647.
Raley R (2013) Dataveillance and Countervailance. In: Gitelman L (ed.), *'Raw Data' Is an Oxymoron*, London, Cambridge University Press, pp. 121–146.
Ramirez E (2013) Larry Smarr: Where There Is Data There Is Hope. *Quantified Self*, Available from: http://quantifiedself.com/2013/02/larry_smarr_croneshope_in_data/ (accessed 13 April 2016).
Rheingold H (2000) *The Virtual Community: Homesteading on the Electronic Frontier*. Cambridge, MIT Press.
Rossi P (1970) *Philosophy, Technology, and the Arts in the Early Modern Era*. New York, Harper Torchbooks.
Saffer D (2014) Why we need to tame our algorithms like dogs. *Wired*, Available from: http://www.wired.com/2014/06/algorithms-humans-bffs/ (accessed 14 April 2016).
Sarewitz D (1996) *Frontiers of Illusion: Science, Technology, and the Politics of Progress*. Philadelphia, Temple University Press.
Seidenberg B (2014) You Should Share Your Health Data: Its Value Outweighs The Privacy Risk. *Wired*, Available from: http://www.wired.com/2014/11/on-sharing-your-medical-info/ (accessed 13 April 2016).
Shapin S (2008) *The Scientific Life: A Moral History of a Late Modern Vocation*. Chicago, University of Chicago Press.

Sharon T (2016) Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. *Philosophy & Technology*, 1–29.

Sharon T and Zandbergen D (2016) From data fetishism to quantifying selves: Self-tracking practices and the other values of data. *New Media & Society*.

Singer E (2011) Quantifying Myself: Self-Tracking Failures. *MIT Technology Review*, Available from: https://www.technologyreview.com/s/424441/quantifying-myself-self-tracking-failures/ (accessed 13 April 2016).

Smarr L (2012) Quantifying your body: A how-to guide from a systems biology perspective. *Biotechnology Journal*, 7(8), 980–991.

Smith ML (1994) Recourse of Empire: Landscapes of Progress in Technological America. In: Smith MR and Marx L (eds), *Does technology drive history?: The dilemma of technological determinism*, Cambridge, MIT Press, pp. 37–52.

Smith MW (2015) A Fitbit fanatic's cry for help: I'm addicted to steps. *The Washington Post*, Available from: https://www.washingtonpost.com/news/to-your-health/wp/2015/05/11/a-fitbit-fanatics-cry-for-help/ (accessed 13 April 2016).

Steyerl H (2016) A Sea of Data: Apophenia and Pattern (Mis-)Recognition. *e-flux*, 72, Available from: http://www.e-flux.com/journal/a-sea-of-data-apophenia-and-pattern-mis-recognition/.

Suchman L (2007) *Human-Machine Reconfigurations: Plans and Situated Actions*. 2nd Editio. Cambridge, Cambridge University Press.

Swan M (2012) Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, 1(3), 217–253, Available from: http://www.mdpi.com/2224-2708/1/3/217/ (accessed 15 July 2014).

Swan M (2013) The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. *Big Data*, 1(2), 85–99, Available from: http://online.liebertpub.com/doi/abs/10.1089/big.2012.0002 (accessed 21 July 2014).

Taking measure of the Quantified Self Movement (2014) *CBS News*, Available from: http://www.cbsnews.com/news/taking-measure-of-the-quantified-self-movement/ (accessed 14 April 2016).

Terranova T (2000) Free Labor: Producing Culture for the Digital Economy. *Social Text*, 18(2), 33–58.

Turner F (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, University of Chicago Press.

Ungerleider N (2014) Why Intel And The Michael J. Fox Foundation Are Teaming Up To Create Wearable Tech For Parkinson's. *Fast Company*, Available from: http://www.fastcompany.com/3034433/why-intel-and-the-michael-j-fox-foundation-are-teaming-up-to-create-wearable-tech-for-parkin (accessed 14 April 2016).

van Dijck J (2013) *The Culture of Connectivity: A Critical History of Social Media*. Cambridge, Oxford University Press.

Wagstaff K (2014) Data Overload: Is the 'Quantified Self' Really the Future? *NBC News*, Available from: http://www.nbcnews.com/tech/innovation/data-overload-quantified-self-really-future-n189596 (accessed 13 April 2016).

Wajcman J and Rose E (2011) Constant Connectivity: Rethinking Interruptions at Work. *Organization Studies*, 32(7), 941–961, Available from: http://oss.sagepub.com/cgi/doi/10.1177/0170840611410829.

Waldman K (2013) The Year We Quantified Everything and Learned … Anything? *Slate*, Available from: http://www.slate.com/blogs/xx_factor/2013/12/27/quantified_self_critique_personal_data_apps_for_calories_exercise_sleep.html (accessed 13 April 2016).

Watson SM (2014) Data Doppelgängers and the Uncanny Valley of Personalization. *The Atlantic*, Available from: http://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780/ (accessed 10 January 2015).

Watson SM (2015) Data is the New '___'. *dis magazine*, Available from: http://dismagazine.com/issues/73298/sara-m-watson-metaphors-of-big-data/ (accessed 12 April 2015).

Winner L (1977) *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, MIT Press.

Wolf G (2009a) Are Self-Trackers Narcissists? *Quantified Self*, Available from: http://quantifiedself.com/2009/02/are-self-trackers-narcissists/ (accessed 5 May 2016).

Wolf G (2009b) Know Thyself. *Wired*, San Francisco.

Wolf G (2010a) QS Show & Tell Tips for Presenters. *Quantified Self*, Available from: http://quantifiedself.com/2010/01/qs-showtell-tips-for-present/ (accessed 1 April 2016).

Wolf G (2010b) The Data-Driven Life. *New York Times*, Available from: http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?_r=1 (accessed 11 January 2014).

Wolf G (n.d.) QS & The Macroscope. *Antephase*, Available from: http://antephase.com/themacroscope (accessed 5 May 2016).

Wolf G and Kelly K (2012) Wired's Gary Wolf & Kevin Kelly Talk the Quantified Self. In: *WIRED Health Conference: Living by Numbers*, New York, Available from: http://library.fora.tv/2012/10/15/Wireds_Gary_Wolf__Kevin_Kelly_Talk_the_Quantified_Self.

Zandbergen D (2013) Data confessions of the quantified self. *Leiden Anthropology Blog*, Available from: http://www.leidenanthropologyblog.nl/articles/data-confessions-of-the-quantified-self (accessed 13 April 2016).

Zilsel E (2000) *The Social Origins of Modern Science*. Raven D, Krohn W, and Cohen RS (eds), Dordrecht, Kluwer Academic Publishers.

Zimmerman J (2014) There's a fitness tracker for vaginas. Quantifying your life has gone too far. *The Guardian*, Available from: http://www.theguardian.com/commentisfree/2014/jul/14/fitness-tracker-vagina-quantified-life (accessed 1 April 2016).

POSTSCRIPT

Bostrom N (2002) Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards. *Journal of Evolution and Technology*, 9.

Dyson E, Gilder G, Keyworth G, et al. (1994) Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. *The Progress and Freedom Foundation*, Available from: http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html (accessed 12 May 2016).

Feenberg A (1991) *Critical Theory of Technology*. Oxford, Oxford University Press.

Haraway D (1991) A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century. In: *Simians, Cyborgs and Women: The Reinvention of Nature*, New York, Routledge, pp. 149–181.

Hörl E (2015) The technological condition. *Parrhesia*, 22, 1–15.

Hu T-H (2015) *The Prehistory of the Cloud*. Cambridge, MIT Press.

Kelly K (2010) *What Technology Wants*. New York, Viking.

Marvin C (1988) *When Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century*. Oxford, Oxford University Press.

Peters JD (1999) *Speaking into the Air: A History of the Idea of Communication*. Chicago, University of Chicago Press.

Peters JD (2015) Life, Death, and Time on the Digital Ship. In: *Digital Existence: Memory, Meaning, Vulnerability*, Sigtuna, Sweden.

Turner F (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, University of Chicago Press.