Lowry P, Dinev T, Willison R.

Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda.

***European Journal of Information Systems* 2017, 26(6), 546-563.**

Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing A Bold Research Agenda

ABSTRACT

In this essay, we outline some important concerns in the hope of improving the effectiveness of security and privacy research. We discuss the need to re-examine our understanding of information technology (IT) and information system (IS) artefacts and to expand the range of the latter to include those artificial phenomena that are crucial to information security and privacy research. We then briefly discuss some prevalent limitations in theory, methodology, and contributions that generally weaken security/privacy studies and jeopardise their chances of publication in a top IS journal. More importantly, we suggest remedies for these weaknesses, identifying specific improvements that can be made and offering a couple of illustrations of such improvements. In particular, we address the notion of loose re-contextualisation, using deterrence theory (DT) research as an example. We also provide an illustration of how the focus on intentions may have resulted in an underuse of powerful theories in security and privacy research, because such theories explain more than just intentions. We then outline three promising opportunities for IS research that should be particularly compelling to security and privacy researchers: online platforms, the Internet of things (IoT), and big data. All of these carry innate information security and privacy risks and vulnerabilities that can be addressed only by researching each link of the systems chain, that is, technologies–policies–processes–people–society–economy–legislature. We conclude by suggesting several specific opportunities for new research in these areas.

KEYWORDS

Security, privacy, information technology (IT) artefact, information systems (IS) artefact, future research, online platforms, the Internet of things (IoT), big data, deterrence theory (DT), rational choice theory (RCT)

1. INTRODUCTION

As senior academicians who have worked diligently as part of the global information system (IS) research community, which has struggled to enrich and promote IS research on security and privacy, there is one question that makes us cringe, as we frequently see it from reviewers and editors of leading IS journals in their responses to security and privacy manuscripts:

'*Where is the IT artefact?*'

Given the long history of security and privacy research in IS, we wonder why this question is still being asked and sometimes used as a sloppy intellectual justification for rejecting papers. Ironically, all three of us have experienced this, including while overseeing this special issue. Certainly, not every security/privacy paper addresses a meaningful information technology (IT) artefact or is relevant to IS research; however, if a paper deals with a substantial security or privacy problem at the organisational level, it is typically highly relevant, not just to IS research but to IS practice.

Accordingly, in this editorial, we address several salient issues. First, we argue that there remains a fundamental misunderstanding of what the IT artefact *is* and of its utility in IS research. This misunderstanding may impede the progress of the entire IS field, not just IS security and privacy research.

Second, there is still a misguided emphasis on the IT artefact, when the proper emphasis should be on the broader *IS artefact*.[1] We are, after all, not IT but IS researchers. We sometimes wonder if members of our field have forgotten about or disagree on what are *information systems* and what is our role in researching them. Third, too many IS researchers have little appreciation for the fact that security and privacy are at the centre of the IS artefact.

We use this editorial to propose a guide for future research, not just for security and privacy researchers, but also for anyone who studies the IS artefact. However, our editorial does not stop merely with rethinking research opportunities related to the IS artefact. We also use this occasion to outline

[1] We expound on this shortly, but basically, we argue that for security and privacy research, this should include anything related to security/privacy that matters or should matter to organisational practice. It does not have to specifically include interactions with a computer.

opportunities for methodological and theoretical improvements that, if implemented, could result in more interesting, influential research and more effective practice. More importantly, we suggest remedies for these weaknesses. We identify specific improvements that can be made to security and privacy research, offering a couple of illustrations. In particular, we challenge the notion of loose re-contextualisation that has gained traction in this research and discuss the example of improving deterrence theory (DT) research. We also explain that the focus on intentions may have resulted in an underuse of powerful theories in security and privacy research, because such theories explain more than just intentions. A proper understanding of the IS artefact actually points to a promising future for IS security and privacy research—precisely because online platforms, the Internet of things (IoT), and big data provide compelling opportunities involving various IS artefacts. We conclude by identifying several specific opportunities for new research in these areas.

2. MOVING FROM THE IT ARTEFACT TO THE IS ARTEFACT

Next, we explain why an obsessive focus on the 'IT artefact' is a potentially undermining and misleading focus that ignores the richness of security and privacy research and practice. We then explain what we mean by 'IS artefact' and why it represents a much more promising way to frame and evaluate security and privacy research.

2.1 Why the IT Artefact Is the Wrong Focus for Security and Privacy Research

Although we believe it is time for the IS research community to move on from its excessive focus on the IT artefact, we commend the thinking and goals that initially drove the IT artefact discussion (e.g. Orlikowski & Iacono, 2001). Indeed, this movement became a focus and de facto standard in IS research because researchers were often attempting to publish research in IS journals in which IS was merely tangentially or superficially addressed, with the result that their papers were in fact psychology, social science, or computer science papers masquerading as IS papers. These practices created an identity crisis in the IS field. It was difficult to know what was and was not IS research, especially because technology topics were increasingly relevant in other academic fields (Benbasat & Zmud, 2003).

The problem that we observe, however, is that reviewers often lack a proper understanding of the IT artefact and interpret it with a crude, black-and-white rubric: for a study to 'count' as IS research, it must involve direct interaction with a specific information system (either hardware or software). Although such interaction with a physical system artefact likely represents the IT artefact, this kind of thinking can result in a regression to a purely positivistic view of science, where that which is unseen is overlooked or considered insignificant or IS phenomena are treated as though they are governed solely by natural laws. We agree with Whinston & Geng (2004), who argued that much of the important research in IS addresses the murky 'grey areas' in respect of the IT artefact. Likewise, we argue, it is the intangible and unseen in IS research and practice that often matters the most—or is at least the most interesting. We thus concur with Lee (1999):

> *'Clearly, if we wish our research to be relevant to practitioners, then we ought to consider doing our research in a way that emulates inquiry in the professions, whether in addition to or instead of doing research in a way that emulates inquiry in the natural sciences' (p. 29).*

This issue is particularly relevant to security and privacy research and practice, because its foundations lie in the 'sciences of the artificial' (Simon, 1996), that is, scientific inquiry that is not fully governed by natural laws because it investigates human-created *artefacts*; in our context, such artefacts include privacy violations, security threats, HIPAA noncompliance, security policies, two-factor authentication, encryption, and so on. Moreover, security and privacy research is interwoven with the constraints of human psychology, law, and professions. Here, the form of inquiry proper to the natural sciences is often the least relevant approach, if not irrelevant altogether, to understanding such human-created artefacts. Pries-Heje & Baskerville (2008) noted the reality of challenging, unstructured managerial decisions, which we believe fit well with security and privacy research:

> *'Perhaps the apex of unstructured decision making occurs in the context of* ***wicked problems****. Such problems are poorly formulated, confusing, and permeated with conflicting values of many decision makers or other stakeholders. Because every outcome of the decision is obscure, the problem cannot be parted or solved piecemeal…* ***Wicked problems*** *share certain characteristics. For example, they can only be formulated in terms of a solution. Their solutions are value-laden, and cannot be denoted true or false, only good or bad. Their solution space is unbounded, and solutions are irreversible'* [emphasis added] (Pries-Heje & Baskerville, 2008, p. 731).

Likewise, organisational security and privacy issues are increasingly 'wicked problems' that call for a rethinking of the key artefacts involved.

2.2 Why the IS Artefact Is the Right Focus for IS Research, and Particularly for Security and Privacy Research

Security and privacy are abstract notions that exist artificially and as a result of legal, organisational (e.g. policy), and cultural mechanisms, which vary by jurisdiction and culture. They are human constructs that we choose to consider important or not. Hence, security and privacy are not even traditional 'IT artefacts' that can be mapped directly to hardware or software artefacts. And yet, it would seem that virtually nothing keeps CIOs awake at night more than their concerns about the security and privacy of their organisations' data. These truly are 'wicked problems', and as such, they are better addressed in terms of a design–theory nexus than as phenomena governed by natural laws (e.g. Pries-Heje & Baskerville, 2008). Online platforms, the IoT, and big data—especially because they intersect—have made security and privacy even more important, such that they are now board-of-director-level and corporate-wide concerns. Aside from the CIO and CTO, there is an increasing cadre of C-level executives dedicated to these issues, such as the chief security officer and chief privacy officer. We argue that a key to this design approach is rethinking the design artefacts associated with security and privacy.

To arrive at our proposition regarding the IS artefact, we take inspiration from Lee *et al.* (2015), who argued that IS design scientists should stop obsessing about the traditional IT artefact and instead focus more clearly on proposing and testing designs that relate to technology artefacts (e.g. hardware or software), information artefacts (e.g. messages), and social artefacts (e.g. a charitable act). We leverage this general idea and propose that it should be extended more widely—to virtually all IS research—and we firmly believe that security and privacy practice brings to light key artefacts that should be accounted for in security and privacy research. We also take inspiration from the editorial direction of *EJIS* itself, which embraces innovative contributions from a diversity of genres (Te'eni *et al.*, 2015).

In doing so, we share the views of Lee *et al.* (2015) and from Currie (2009), who maintained that there needs to be a better distinction between the IT artefact and its context, which could include

organisational, social, and environmental factors of a system's implementation. From a security and privacy perspective, this refined distinction also means that important security and privacy phenomena or outcomes are artefacts that should be of central interest to researchers. Again, such artefacts derive from the 'sciences of the artificial', such that they are not governed by natural laws of nature but are created by humans and organisations (Simon, 1996). We thus believe that several additional key artefacts are highly relevant and should be studied in security and privacy research:

- process artefact
- organisation artefact
- person artefact
- threat artefact
- legal artefact
- protection artefact
- vulnerability artefact
- a broadly conceived social artefact, including culture

Although not all of these artefacts apply to every subfield of IS research—threat, protection, and vulnerability primarily apply only to security and privacy research—we believe that the underlying principle of better analysis through the contextualisation of artefacts will make for better and more interesting IS research. Indeed, IS research that focuses solely on hardware or software considerations turns out to be less interesting. As an interdisciplinary field that investigates intersections between hardware, software, people, cultures, organisations, and information, we believe it is in these intersections that interesting and meaningful IS security and privacy research emerges. As further elaboration, in Table 1 we present some key examples of security and privacy studies from the last 10 years, from which we have derived key IS artefacts that are relevant to security and privacy researchers.

Table 1. Non-exhaustive Examples of IS Artefacts that are Pivotal to Security and Privacy Research*

Our Proposed IS Artefact (Definition)	**Example of the Artefacts in Security or Privacy Context**	**Citation Support**
Ethics artefact (considerations and decisions regarding the rational application of the morality of organisational decisions that directly	Discourse ethics applied to information, security or privacy	Myyry *et al.* (2009); Mingers & Walsham (2010); Chatterjee & Sarker (2013); Lowry *et al.* (2014); Chatterjee *et al.* (2015)
	Situational ethics applied to security/privacy; for example, personal rationalisations of violations or corporate violations of security/privacy rules under strain	Myyry *et al.* (2009); Siponen & Vance (2010); Wall *et al.* (2016)

involve security or privacy)	Rational morality and ethics as security/privacy violation deterrence mechanisms	D'Arcy *et al.* (2009); Bulgurcu *et al.* (2010); D'arcy & Herath (2011); Li *et al.* (2014)
	Cross-cultural differences in information ethics	Martinsons & Ma (2009); Lowry *et al.* (2014)
	Organisational level privacy programs based on ethical reasoning.	Culnan & Williams (2009)
Information artefact (phenomena involving the nexus between security/privacy and data, information, knowledge, or communication)	Big data	Davenport *et al.* (2007); Menon & Sarkar (2016)
	Information security policy documents or manuals	Siponen & Willison (2009); Bulgurcu *et al.* (2010); Cram *et al.* (2017)
	Phishing email messages Spoofing web sites/emails	Wright *et al.* (2014); Zahedi *et al.* (2015); Wang *et al.* (2016); Goel *et al.* (2017); Moody *et al.* (2017); Wang *et al.* (2017)
	Security warning messages	Anderson *et al.* (2016)
	Social engineering attempts	Workman (2007); Algarni *et al.* (2017)
	Spam	Caliendo *et al.* (2012)
Legal artefact (phenomena involving the nexus between security/privacy and law, regulations, policy, or best practices)	HIPAA or PCI violations	Wall *et al.* (2016)
	Regulatory approach to privacy	Culnan & Williams (2009); Miltgen & Smith (2015); Wall *et al.* (2016)
	Theft of intellectual property or digital goods	Bauer *et al.* (2016); Lowry *et al.* (2017b)
	Transnational data flows	Hui *et al.* (2017)
Organisational artefact (organisation-level phenomena that directly involve security/privacy as they affect organisations)	Board-level IT governance of security and privacy strategy	Turel & Bart (2014); Lee *et al.* (2016)
	Extra-role organisational behaviours for security and privacy	Hsu *et al.* (2015)
	Security and risk-prevention investments by organisations	Chen *et al.* (2011); Angst *et al.* (2017); Baskerville *et al.* (2017)
	Self-regulation Privacy policies Fair information practices Privacy assurance	Hui *et al.* (2007); Tang *et al.* (2008); Lowry *et al.* (2012); Bansal & Gefen (2015); Gerlach *et al.* (2015); Greenaway *et al.* (2015); Parks *et al.* (2017)
	Top management commitment to security and privacy Standards and best practices	Herath & Rao (2009b); Hu *et al.* (2012); Lee *et al.* (2016); Niemimaa & Niemimaa (2017)
Person artefact (phenomena involving rational/irrational thought, dispositions, habit, emotion, and cognition involving information privacy/security)	Behavioural economics vs rational decision Affective responses	Angst & Agarwal (2009); Tsai *et al.* (2011); Acquisti *et al.* (2012); Goes (2013); Dinev *et al.* (2015); Burns *et al.* (2017b)
	Mindset of the cyberbully	Lowry *et al.* (2016b); Lowry *et al.* (2017a)
	Mindset of the hacker	Dey *et al.* (2012)
	Mindset of the insider vs the security professional	Posey *et al.* (2014)
	Privacy calculus	Xu *et al.* (2010); Keith *et al.* (2013); Keith *et al.* (2016); Kordzadeh & Warren (2017); Kokolakis (2017)
	Privacy correlates: anonymity, secrecy, awareness	Dinev *et al.* (2013); Li & Qin (2017)
	Security awareness of employees	D'aubeterre *et al.* (2008); D'Arcy *et al.* (2009)
	The brain's response; neuroIS approach	Anderson *et al.* (2016); Warkentin *et al.* (2016)
	Anonymising and sharing key security and privacy information between organisations	Li & Qin (2017); Vance *et al.* (2017)
	Effective IT auditing	Merhout & Havelka (2008)

Process artefact (process or procedure phenomena that involve privacy/security configuration, governance, or risk management)	Information security management, risk management, and governance	Veiga & Eloff (2007); Spears & Barki (2010); Tsohou *et al.* (2015)
	Privacy impact assessments	Oetzel & Spiekermann (2014)
	Privacy/security balance with identity ecosystems	Crossler & Posey (2017)
	System configuration failures	Chen *et al.* (2011)
Protection artefact (messaging, training, and persuasion phenomena designed to encourage individual-level protective security/privacy behaviours)	Fear appeals	Johnston & Warkentin (2010); Boss *et al.* (2015); Johnston *et al.* (2015)
	Protection behaviours	Dinev *et al.* (2009); Posey *et al.* (2013); Posey *et al.* (2015); Burns *et al.* (2017b)
	Resistance to phishing attempts	Wright *et al.* (2014)
	SETA initiatives	Luo & Liao (2007); D'Arcy *et al.* (2009); Karjalainen & Siponen (2011); Tsohou *et al.* (2015)
Social artefact (social, cultural, organisational, and group-level phenomena involving security/privacy)	Cultural influences on security and privacy behaviours	Dinev *et al.* (2009); Lowry *et al.* (2011)
	Employee data leakage on social media	Huth *et al.* (2013)
	Employee neutralisation and rationalisation of bad behaviour; negative social influence	Siponen & Vance (2010); D'Arcy *et al.* (2014)
	Negative employee reactance against threatening information security policies	Lowry & Moody (2015)
	Sense of justice and fairness in security and privacy policies	Lowry *et al.* (2015)
Technology artefact (tangible phenomena involving the nexus between security/privacy and physical computing equipment, software, networks, or interfaces)	Computer abuse Physical destruction of property	Willison & Warkentin (2013); Lowry *et al.* (2015)
	Encryption standards and applications	Heikkila (2007)
	Equipment theft	Veiga & Eloff (2007); Willison & Warkentin (2013)
	Interface design to prevent security/privacy issues	Vance *et al.* (2015); Lowry *et al.* (2017a)
	Firewalls	Cavusoglu *et al.* (2009)
	Location-based services	Xu *et al.* (2010); Keith *et al.* (2013)
	Lost USB device with highly confidential information	Heikkila (2007)
Threat artefact (natural, unintentional, or intentional danger phenomena that have the potential to harm an organisation, system, or individual in respect of security/privacy)	Access policy violations	Vance *et al.* (2015)
	Click fraud	Dinev *et al.* (2008); Chen *et al.* (2015)
	Data breaches Privacy invasions	Culnan & Williams (2009); Choi *et al.* (2015); Angst *et al.* (2017); Goode *et al.* (2017); Karwatzki *et al.* (2017); Ozdemir *et al.* (2017); Posey *et al.* (2017)
	Denial-of-service attacks Cyberattacks	Ransbotham & Mitra (2009); Kim *et al.* (2011); Hui *et al.* (2017)
	Insider threats	D'Arcy *et al.* (2009); Warkentin & Willison (2009); Hu *et al.* (2011); Wang *et al.* (2015a)
	Malware and spyware Ransomware	Luo & Liao (2007); Lee & Larsen (2009); Boss *et al.* (2015)
	Rootkit infection	Beegle (2007)
Vulnerability artefact (tangible or intangible weakness or gap	Bring your own device (BYOD)	Crossler *et al.* (2014)
	Cloud-computing adoption	Paquette *et al.* (2010); Subashini & Kavitha (2011)

phenomena that expose an organisation, system, or individual to security/privacy risks)	Hardware failure that reveals attack vulnerability	Sumner (2009)
	Security/ privacy policy violations	Herath & Rao (2009b); Siponen & Vance (2010); Hu *et al.* (2011); Vance *et al.* (2015); Johnston *et al.* (2016)
	Unpatched operating systems	August & Tunca (2008)
	Untrained or careless employees	Wright *et al.* (2014)
	Vulnerability management	Chen *et al.* (2011); Baskerville *et al.* (2017)
	Risk in online information disclosures	Posey *et al.* (2010); Gefen & Pavlou (2012); (2015); Wang *et al.* (2015b)

*Note: Our literature examples are from the last 10 years, focusing on IS and technology journals. Aside from these key security/privacy artefact ideas we derived from the recent literature, we also encourage the reader to consider several review articles from which other IS artefacts relevant to security/privacy may be derived, including Bélanger & Crossler (2011); Pavlou (2011); Smith *et al.* (2011); Crossler *et al.* (2013); Willison & Warkentin (2013); Cram *et al.* (2017).

A key issue we want to head off in advocating an IS-artefact view of security and privacy research is that these factors should not be treated as a necessary check list. That is, a valid IS security study should not have to exhaustively address each of these artefacts in one study, which would be excessive and unrealistic. Addressing one or more of these should be sufficient for a study to make a focused, meaningful contribution. However, the bigger issue is whether the researcher is addressing a security or privacy issue that organisations care about or would care about if they knew better.

3. OTHER ASPECTS OF GOOD PRIVACY/SECURITY RESEARCH

Clearly, a security or privacy study is not appropriate for a top IS journal merely because it properly addresses an important IS artefact. Other consistent standards still apply. Before we send security and privacy papers out for review at our journals, we first ask questions like the following: Is there native IS theory development or original contextualisation of an outside theory? Are the findings novel, surprising, and exciting? Will the findings, if widely disseminated, likely change the way researchers look at the problem going forward, and do the findings provide an opportunity to improve practice? Are the methods well executed and reasonable? Does the study have *ecological validity*[2] and yet go beyond restating the obvious in respect of what managers already know?

[2] Ecological validity should not be confused with external validity. *Ecological validity* indicates the degree to which findings of a research study can be generalised to *real-life settings*, often because they are collected or generated in real-life settings (e.g. actual employees trying to solve real work tasks) (Brewer, 2000). Although this form of validity—unlike internal and external validity—is not strictly required for a study to be valid, it is a

Although we cannot fully describe what good security and privacy research is, we can easily describe what it is not. Although every study suffers from trade-offs and limitations and one or two key weaknesses, a weak study suffers from several limiting factors, all of compound to create the universally dreaded (albeit sometimes imaginary) 'fatal flaws'. A weak study will likely exhibit one or more of the characteristics summarised in Table 2, typically in multiple combinations. Here, we focus on factors we believe are especially pertinent to organisational security and privacy research, although many of these factors and solutions apply in other contexts. We also follow the *EJIS* principle of embracing the best of a diversity of genres (Te'eni *et al.*, 2015).

Table 2. Indicators of a Potentially Weak Security/Privacy Study and Possible Solutions

Category	Indicator of Weakness	Solution
Contribution	A lack of face validity or ecological validity in the results such that they are not useful or violate common sense in practice	We argue that ecological validity (e.g. realism) (Brewer, 2000) is especially pertinent for security and privacy research, because for such research to have meaningful influence, its corresponding solutions should work effectively with actual people in real organisations.
Contribution	A sense that the findings are 'obvious' and already known (Rai, 2017)	Rather than starting security/privacy studies based on gap-spotting the literature (Alvesson & Sandberg, 2011) or applying a known theory in a new context, focus more on a controversial, pressing problem in research or practice (Rai, 2017).
Contribution	A sense that the problem is 'made up' or not pressing (Rai, 2017)	This typically occurs as a result of gap-spotting the literature (Alvesson & Sandberg, 2011) to find problem opportunities without consideration of the living academic community or practice community. The easiest solution is to take a more *engaged scholarship* approach, that is, to bring together the scholarly literature, discussions with scholarly experts, and connections with practice to identify problems that are real and pressing (Van de Ven, 2007). True engaged scholarship follows this principle not just in problem identification but in theory building, construct and measurement development, data collection, and interpretation of findings.
Contribution	Results that seem implausible or overly 'convenient'	Provide transparency on pilot tests, theory development, and instrumentation development, and avoid *model trimming* (e.g. dropping constructs and relationships that are insignificant in a large model) unless it is done under the direction of a knowledgeable review team and for the purpose of theoretical parsimony. Nonetheless, any such directed trimming should be documented to better support future replications, meta-analyses, and scientific transparency.
Methodology	Building new measures solely from the literature	Practice engaged scholarship within communities of practice and research in measurement development (Van de Ven, 2007).

particularly meaningful but often overlooked consideration for research areas that are highly intertwined with practice, such as security and privacy research.

Methodology	Focusing on intentions or hypothetical vignettes alone	Where possible, gather self-reported or actual observed security/privacy behaviours (e.g. Keith *et al.*, 2013; Boss *et al.*, 2015). Triangulate an intentions study with behaviour data or secondary data. Use vignettes for proof-of-concept and then follow up with field experiment.
Methodology	Lack of true control and treatment groups	Even in field research, use controls and treatments to establish causation (Boss *et al.*, 2015; Johnston *et al.*, 2015).
Methodology	Paper-based, one-off, cross-sectional study	Longitudinal data collections; use of electronic instead of paper-based data-collection methods to improve data quality (Lowry *et al.*, 2016a); use of mixed methods (e.g. self-report with secondary data).
Methodology	Student sampling or sampling from one organisation	Sampling from multiple organisations or through leading online panels (Lowry *et al.*, 2016a).
Methodology	Overreliance on self-reported measurement	Triangulation of self-report measurement with objective, observed measurement of actual security/privacy behaviours in which the participants do not know they are being observed (Keith *et al.*, 2013; Keith *et al.*, 2015); multilevel measurement involving self-report and report by one's manager or peers (Hsu *et al.*, 2015); use of secondary datasets for additional organisational-level measurement (Kwon & Johnson, 2014).
Theory	Amalgamations of theory mixed in with seemingly random constructs that are put together into what the authors call a theoretical model (Hassan & Lowry, 2015)	Although IS researchers certainly need not be beholden to established theories, and should definitely create new sociotechnical theories to explain the science of the artificial (Simon, 1996), these still need to have a coherent underlying story, involving related and meaningful causal mechanisms (Hassan & Lowry, 2015).
Theory	Questionable measurement, construct validity, and content validity (Bagozzi *et al.*, 1991)	We consider this a theory problem, because constructs come from theory, and measurements should be chosen to properly represent the actual meaning of the constructs (Bagozzi *et al.*, 1991). Otherwise, a study will suffer from lack of content or construct validity, and thus the empirical data will not properly test the underlying theory.
Theory	Weakly applied theorisation in which theory is loosely borrowed without due consideration to its underlying assumptions and without properly re-contextualising it (Whetten *et al.*, 2009)	Many opportunities still exist to borrow and adapt key theories from reference disciplines, such as criminology and sociology. Indeed, good theorising is highly contextualised (e.g. Whetten *et al.*, 2009), and this is especially true in security and privacy research (e.g. Boss *et al.*, 2015; Wall *et al.*, 2016). However, before adapting and modifying a theory, it is crucial to understand its boundary conditions, assumptions, constructs, and casual mechanisms. In doing so, researchers can thus better explain, justify, and motivate adaptations that are different from the originals as well as demonstrate why they are useful.

Pointedly, we admit to publishing research that suffers from some of the above weaknesses. In fact, many researchers are 'coerced' into these narratives as a matter of pre-tenure survival. But what we have found is that research that goes beyond these simple approaches tends to be better received at top journals and has more impact. We have especially noticed in security and privacy research a tendency

among authors to push ideas out to journals quickly[3] and to perhaps over focus on preliminary-style studies involving intentions with self-report cross-sectional surveys. Although this is certainly a valid approach, especially when exploring a new topic area or for mere career survival—after all, many of us live in a publish-or-perish paradigm in which we do not have the luxury of refining a theory for 10 years—we find this to be an increasingly limited approach to making meaningful contributions in a mature area of research. We believe that, as any area matures, the more effective way to contribute to science (and then survive by publishing in top journals) is to enhance the novelty or rigor of the methods, the novelty or explanatory power of the theory, and the novelty of the research questions.

For example, it is particularly easy to conduct a factorial survey method study using Amazon Mechanical Turk participants examine participants' intentions to comply with their company's ISPs. By contrast, it is particularly difficult to conduct such a study in an ecologically valid setting in which participants across hundreds of organisations are tracked for their ISP compliance (not just through self-report but perhaps through automated report or report from their supervisors) in a longitudinal study. Although the latter approach is indeed more difficult (and impossible in many settings), it can provide more ecological validity—by showing how employees' cognitions and behaviours change over time, how effective training interventions develop over time, how to better interact with day-to-day organisational practice, and so on.

However, we recommend the use of common sense in judging the level of evidence required for a given security/privacy study. To be fair, there is a big difference between studying illegal behaviour and noncompliance/compliance behaviour. As a rule, organisations will not allow the study of illegal behaviour, whereas they will more frequently allow the study of noncompliance/compliance behaviour. Some problems are so 'wicked' they present serious legal challenges to organisations—and even create

[3] To help address this issue, the *Dewald Roode Workshop in Information Systems Security Research* was started in 2009, as sponsored by IFIP WG 8.11 / 11.13, to help security and privacy researchers prepare articles for submission to top journals. Likewise, the AIS sponsors SIG-SEC, which hosts key security/privacy workshops before top AIS conferences, such as ICIS. We urge the security/privacy community to leverage such opportunities before submitting to journal, and at a minimum to circulate manuscripts among their colleagues.

liabilities for researchers—and thus can be studied only through intentions, surrogate measures, or secondary data. Conversely, because many organisations have enhanced their auditing and risk management practices, they are increasingly providing opportunities to study actual compliance behaviour. Thus, researchers are starting to work with organisations and third parties to conduct penetration testing, simulate phishing attacks, and the like. These are compelling data-collection opportunities.

In the remainder of this section, we further illustrate specific improvements that can be made with a couple of in-depth illustrations that we believe can dramatically improve security and privacy research. First, we challenge the notion of loose re-contextualisation that has gained prominence in this field of study and provide an example of DT research. Second, we provide an illustration of how the focus on intentions has undermined the use of powerful theories in security and privacy research, because the theories were designed to explain phenomena other than intentions. In the next section, we continue to lay out a promising agenda for new avenues of security and privacy research.

3.1 Improving the 'Contextualisation' of Reference Theories: The Example of Deterrence Theory

Like every other scientific field, IS research has strengthened and expanded its theoretical foundations by applying reference theories and associated concepts and from other fields. For example, in explaining employees' abuse of computer and information resources, a number of papers in IS security research have drawn theories from the field of criminology. This exercise has brought significant contributions and new perspectives to IS security research. Where better to gain insights into criminal behaviour than from a field that places the understanding of offender behaviour centre-stage?

From a security perspective, DT was first applied by Straub (1990). Many exemplary papers have since examined criminal internal computer abuse (ICA) (e.g. Harrington, 1996; Peace *et al.*, 2003; Lee *et al.*, 2004; Workman, 2007; Hu *et al.*, 2011; Posey *et al.*, 2011; Lowry *et al.*, 2014; Lowry *et al.*, 2015; Willison *et al.*, 2017). Whereas some studies have focused only on criminal behaviour, others have investigated noncriminal behaviour as well (e.g. Siponen *et al.*, 2007; Herath & Rao, 2009b, 2009a; Bulgurcu *et al.*, 2010; Son, 2011; Chen *et al.*, 2013). Thus, in our example of improving

contextualisation, we consider the use of DT for criminal and noncriminal settings, and possibly a mix of the two.

As we attempt to uncover exciting research opportunities by re-contextualising theories from other disciplines, it may be good to start by going back and asking ourselves what exactly we mean by 're-contextualisation'. Whetten *et al.* (2009) and Boss *et al.* (2015) suggested that proper re-contextualisation involves more than merely adapting the measures associated with a theory to a new context; it involves a critical understanding of how the assumptions of a theory might work in a new context and making carefully documented and supported adaptations, as necessary. DT provides an excellent illustration of this opportunity. With its origins in criminology, DT asserts that in committing a crime, a potential offender will consider the costs associated with legal punishment. More specifically, if the chances of being caught are high (i.e. sanction certainty), the associated penalties severe (i.e. sanction severity), and the punishment swift (i.e. sanction celerity), then the potential offender will be dissuaded from committing the crime.

A focal point in the seminal DT writings of Bentham (1988), Beccaria (2009), Andenaes (1952), Becker (1968), and Gibbs (1975) is the potential deterrence effect of the criminal justice system. Some criminologists would thus likely question extending DT to noncriminal contexts.

However, we believe that DT could potentially be fully re-contextualised to noncriminal contexts, given that the assumptions and boundary conditions of DT are clearly and transparently laid out. Theorists could thus use further logic, evidence, and metaphors to carefully explain and justify the use of DT in noncriminal contexts. Accordingly, this could be an excellent opportunity for security and privacy researchers to fully rework and reshape DT and establish theoretical ownership over a different version of DT that is fully contextualised. This kind of re-contextualization was advocated by Whetten *et al.* (2009) and painstakingly demonstrated by Wall *et al.* (2016) in an organisational security/privacy theory-building paper. In that respect, an excellent research opportunity would be for security and privacy researchers to explain how and why organisational sanctions in an organisational security context can act as effective and are legitimate replacements of the formal criminal justice system in classical DT models.

Likewise, it would be important to better understand what kinds of non-legal formal and informal sanctions work best with various kinds of security/privacy behaviours, and again, *why*.

Another compelling departure from the criminological strictures of DT has been the use of DT to examine *positive behaviour* in the form of employee compliance with organisational information security policies (e.g. Siponen *et al.*, 2007; Herath & Rao, 2009b, 2009a; Bulgurcu *et al.*, 2010; Son, 2011; Chen *et al.*, 2013). Such studies have offered fascinating empirical evidence, and this evidence is contrary to what criminologists would expect. A further contribution of security and privacy research could be to conduct more studies to explain *why* DT works so well in promoting positive behaviours and what the limitations may be. Here, we thus see the conversation as just starting.

3.2 Moving away from Intentions, When It Is Feasible

With the aim of reorienting IT adoption research, Benbasat & Barki (2007) offered their views in a paper entitled 'Quo vadis, TAM'? As the title suggests, their concerns related to the technology acceptance model (TAM) (Davis *et al.*, 1989). Although Benbasat and Barki acknowledged the success of TAM, they also maintained that it has produced several 'dysfunctional outcomes'. What is interesting about these outcomes is how many of them have also occurred in security and privacy research. Although TAM has not been widely applied in security and privacy research, the common denominator between TAM and our field is the intentions construct. We thus note the greater opportunity for security and privacy research to move beyond the intentions construct in an attempt to study actual behaviour and to better understand the decision-making process related to security/privacy behaviours.

To illustrate this opportunity, we consider studies that have focused on ICA. The extent to which the actions under investigation can be considered 'abusive' varies from paper to paper, with some studies addressing relatively benign behaviour and others more malicious. Some of the studies involve intentions, and some involve reported behaviours or actual observed behaviours.[4] A key opportunity in all of these is

[4] Some ICA studies have effectively used scenarios in a bid to 'place' respondents in a lifelike situation (e.g. D'Arcy *et al.*, 2009; Hu *et al.*, 2011; Willison *et al.*, 2017) where they do not have to admit directly to illegal behaviour. These are certainly useful approaches for understanding such behaviour, but such scenarios underplay the influence of offenders' skills and abilities, the context in which they work, and the relationship between them.

to further delve into a person's *decision-making process* for security/privacy violations or compliance. For example, criminological research has acknowledged that offenders make a series of choices in the criminal decision-making process (Blumstein *et al.*, 1988; Hagan, 1997; Sampson & Laub, 2005). Namely, the rational choice perspective advanced by Clarke & Cornish (1985) posits that offenders make a series of choices related to specific stages of the criminal decision-making process. Do these arguments apply to ICA, and do they apply to noncriminal decisions such as those related to security policy compliance/noncompliance? This question points to rich re-contextualisation and methodological opportunities for security and privacy researchers.

Aside from noting the absence of research into the motivations of ICA or noncriminal policy violation, we also believe that the current approach of examining intentions as a proxy for behaviour in security and privacy research may be too limiting. When considering the organisational context, we can follow the example of the criminology theories, including environmental criminology (Brantingham & Brantingham, 1991), routine activity theory (Felson, 1994), and the rational choice perspective (Clarke & Cornish, 1985), which have shown that potential criminal opportunities also depend on the offender's skills and abilities required to perform the crime, the offender's knowledge of potential safeguards, and other factors. For example, an accountant in an organisation will have the skills and access necessary for electronic bookkeeping. Through a knowledge of security vulnerabilities, the employee, if motivated, may decide to perpetrate fraud. However, a member of the marketing department would be unlikely to have access to the bookkeeping system or the ability to perform a similar crime. However, the marketing employee may have access to customer data, which could equally be misused or defrauded. This example demonstrates that what constitutes an ICA opportunity for an employee in one department may not constitute such an opportunity for a member of a different department. Likewise, there likely exists an intentions–behaviour gap in respect of security/policy compliance behaviour as well. It is easy to 'intend' positive behaviour, but actual compliance can take substantial effort, which can undermine one's work productivity or create other costly nuisances.

To be clear, there are good justifications for using intentions data in research, especially in newer areas of security and privacy research or in cases where it is the only feasible way to gather data (e.g. studies of highly illegal behaviour). We also recognise that organisation-level security/privacy data is among the data most difficult to gather, such that most organisations refuse access to such information, especially for criminal violations. We thus see studies of behavioural organisational security/privacy more as a 'Holy Grail' or aspirational goal for security and privacy research than as a required standard. Nonetheless, actual behavioural data can be easier to gather in other settings, such as with consumers' use of smartphones, social networking studies, and the like. We simply encourage researchers to strive to use the best sources they can and to think outside the box—but we also encourage editors and reviewers to be thoughtful and realistic in their expectations for empirical evidence.

4. PROMISING FUTURE RESEARCH: SECURITY AND PRIVACY AT THE CENTRE OF THE IS ARTEFACT

Turning from a more critical review of how we can improve what we are already doing in security and privacy research, we now take a more positive view by laying out unexploited, exciting opportunities that put security and privacy at the centre of the IS artefact by focusing on (1) online platforms, (2) the IoT, and (3) big data. Importantly, these three often intersect and thus further complicate security/privacy issues.

4.1 Opportunities in Online Platforms

We believe that online platform markets represent one of the bigger IT transformations that has occurred since the emergence of the Internet (cf. Parker *et al.*, 2017; Song *et al.*, 2017). These markets are obliterating traditional e-commerce, retail, and supply chains. The key to their emergence is the interesting delivery of core economic principles related to demand-side economics, supply-side economics, and network economies of scale and scope. Platforms have arisen because the market 'increasingly favours orchestration [of third-party content providers] over [in-house] production' (Parker *et al.*, 2017, p. 255). Likewise, platforms are more likely to enable economies of scale (Krishnan & Gupta, 2001; Bakos & Katsamakas, 2008). As a result, we have new kinds of interconnected technologies

and business models that are based on platforms, and platform-based businesses are among the most profitable on the planet (e.g. Google, Amazon, Taobao, Tencent, Uber, Facebook, Apple, AirBnB).Consider the degree to which Amazon has affected retail markets throughout the world. Amazon provides a platform-based, fully integrated service that allows for the delivery of over 50 million items in free two-hour, same-day, or two-day delivery schemes. No physical store can compete with such selection and velocity. As a result, major traditional retailers have been forced to respond and adapt at a fast pace, and some (e.g. Walmart) have raced to create their own platforms. Those that have not (e.g. Macys, Nordstrom, Aeropostale, Sears Holdings Corporation—owner of K-Mart) are facing dire consequences.[5] Clearly, we are moving to a platform-based world. However, the race to create and implement these online platforms has provided little time to consider unintended caveats and risks when it comes to both security and privacy. The complexity of these systems is significantly greater than the systems we have known before because of the scale and scope of their interactions (Burns *et al.*, 2017a). Consider the inventory and shipping complexity of Amazon's 50 million distinct stock keeping units. For leading platforms to work well, they must tie together massive supply chains throughout the world, with larger, more heterogeneous groups of customers than was possible before. To win, online platforms need massive scale and scope, with network effects that dramatically drive down marginal costs (Armstrong, 2006; Rochet & Tirole, 2006). It is troubling to the status quo that the market favours natural monopolies and 'tips' toward platforms of the largest economies of scale and scope, which have huge network effects, resulting in 'winner-take-all' markets (Liu *et al.*, 2011). But this kind of complexity, scale, and size makes for systems that have even greater vulnerabilities to security and privacy issues. They are also greater targets for external and internal threats. Attackers may concentrate their efforts on the few organisations in the world that can win at the 'winner-take-all' platforms. If the attackers are successful, the organisations and the consumers can suffer significant losses in terms of security and privacy. If a critical point is reached, an irreversible erosion of consumer trust in these platforms can set in, driving

[5] To wit, given the platform revolution's disruption on traditional retailers, *Forbes* recently boldly declared, 'Traditional retail might not be dead, but it is in a coffin' (Lavin, 2017).

down consumer willingness to transact on them. The September 2017 Equifax breach represents such a worse-case scenario, in which hackers continually focused on a treasure trove of private information until they were successful.

Such platforms also facilitate the use of new transaction technologies, especially e-payment, which have disrupted the natural order of banks acting as middle-men for payment transactions. These also create new privacy, security, and trust relationships (Tsiakis & Sthephanides, 2005; Kim *et al.*, 2010). For example, consumers can disintermediate traditional banks and pay directly through Alipay™, WeChat Pay™, PayPal™, Apple Wallet™, Google Wallet™, and so on. Such disintermediation further fosters online platforms, and it exposes consumers and governments to new security/privacy risks, especially as untraceable cyber/crypto currencies emerge, such as bitcoin, as facilitated by block chain technology (Karame, 2016; Underwood, 2016).

Following news and social media, consumers have become increasingly aware of the security risks and the massive personal data collection and data sharing conducted by these platforms. Furthermore, they have come to the realisation that we are all vulnerable and it is increasingly difficult to opt out of this global system or for any of our activities to remain private. This is especially true as natural monopolies and oligopolies are formed. Who, for example, can opt out of Google Scholar™ and stay abreast of the latest research? Consequently, any consumer and organisation will have to worry not only about home-grown systems, but about the system at large as well. A Walmart supplier is vulnerable to Walmart and its thousands of other interconnected suppliers. Google is embedded in one form or another in most of the world's systems, whether by mobile phone, search, email, GPS and mapping, or storage technology. The 2013 Target data breach, which affecting 41 million customers, may be a worst-case example here. This was a platform-based breach, based on a successful phishing email to a third-party system. Based on information from the third party, hackers gained access to Target's customer service database, on which they installed spyware that captured highly private customer data.

Consequently, online platforms provide rich opportunities for research, particularly in terms of shedding serious academic light on the security and privacy issues. It is challenging to be more specific,

because the research ideas and creativity of the IS community are boundless. Nevertheless, solid academic studies on security and privacy in online platforms are sure to be impactful and increasingly compelling.

4.2 Opportunities in the Internet of Things

Like online platforms, the IoT, which is the internetworking of various physical devices, is rewriting all the rules we once had about organisational security and privacy. We now live in a world in which there are more automatic 'things' than there are people. Hence, the IoT will naturally extend platforms, dramatically complicating the underlying security and privacy issues. Unfortunately for IT security and privacy professionals, these 'things' are multiplying exponentially. Bring your own device (BYOD) initiatives have already become a security and privacy nightmare for organisations (French *et al.*, 2014; Garba *et al.*, 2015). The IoT entails the same nightmare as BYOD, but exponentially increased. This is particularly true because the key to most of this internetworking is an architecture of wireless transmitters and sensors that will connect into vast global, networks. These range from the smallest of transmitters and passive RFID chips to directly wired applications such as home automation apps. Hence, the IoT affects everything from online platforms and wearable technologies to automated cars and planes. Accordingly, the IoT is progressing much more rapidly than are security and privacy standards, causing many gaping security holes (Singh *et al.*, 2015), especially because security/privacy policies are often engineered after the fact. For one, there are conflicting communication protocols, each of which has its own security loopholes. For another, current organisational practices for managing security, such as the use of firewalls, routers, and gateways, simply do not work for smaller and more mobile 'things'. The IoT gives even more creative and nefarious opportunities for hackers that were not possible before, such as spying on someone through their refrigerator, listening to someone through their smartphone, turning off a home thermostat to cause the pipes to freeze and burst overnight, attacking someone's pacemaker or insulin pump (Burns *et al.*, 2016), unlocking the Bluetooth locks for households,[6] suddenly locking a

[6] Bluetooth is especially prone to 'man-in-the-middle attacks' because of security flaws of the Bluetooth protocol itself. Hackers can easily intercept the transmitted data and can spoof device behaviour for authentication.

car's brakes at high speed, sending a drone into traffic, and so on. In fact, such destructive possibilities may forever change the security profession such that many security professionals will have to act in roles of deception and counterintelligence to stay ahead of attacks.

As indicated by the examples discussed above, through the IoT, the physical security and well-being of people and their homes are increasingly tied to the network and information system's health and security. Hence, information security and privacy breaches are no longer abstract notions or a danger only for big organisations or for remote personal data sitting somewhere in a database. Rather, these breaches increasingly hit consumers in their homes and daily lives (e.g. smartphones). We can easily imagine the apocalyptic security/privacy consequences of breaching a network of millions of smart automobiles speaking to each other and to traffic sensors through a mesh of sensor networks and other 'smart' devices.

Even if no breach occurs, the sheer amount of data gathered from IoT devices may concern consumers. MIT professor Alex Pentland noted in his interview with the *Harvard Business Review* staff (Berinato, 2014) that even the data points by which people's daily behaviour is gathered may make people feel invaded. 'As sensors are built into more and more products, there's a sense of being increasingly spied on' (p. 102). The IoT's vulnerability to security/privacy attacks and even life-threatening breaches on individuals' systems or data can affect virtually everyone. Thus, as the use of the IoT matures, we expect a societal wave of changes in terms of how people think about using networked devices and applications and who controls the data. If the use of the IoT turns out to be disaster prone, with people dying as a result, there will be calls to shut down the IoT, with drastic regulations passed overnight (Pentland, in Berinato, 2014). Thus, the IoT is the ultimate example of the IS artefact vs the IT artefact argument: whereas most technologists are excited about the creative technical possibilities the IoT can bring to our lives, only the social and organisational scientists, with consistent and disciplined

Hence, all Bluetooth-enabled devices, from locks to smart watches and medical instruments, are highly susceptible to attacks. A large number of academic studies have confirmed such holes and suggested remedies (Hager & MidKiff, 2003; Haataja & Toivanen, 2010), but the devices continue to be exploited because of the protocol's fundamental design.

'systems' thinking, can, when 'things' go awry, thoroughly and deeply reveal the technologies–policies–processes–people–society–economy–legislature chain of cause and effect.

4.3 Opportunities in Big Data

We now live in a world in which we are overwhelmed with data, and data is increasingly needed for strategic advantage. As a result of the data-gathering capabilities of platforms and the IoT, technological and business advances in data aggregation and business intelligence (Chen *et al.*, 2012), and changing societal and cultural norms that favour the sharing of personal information, this data is increasingly 'big'. It is generated in ever-increasing volumes, at increasing speed, and in increasing variety (e.g. text, sound, video, blog). Because of the massive size of this data, it often cannot be stored on traditional corporate servers, but instead requires increasingly massive, outsourced server farms in what is commonly referred to as 'the cloud'. In reality, these are simply data centres run by third parties, which usually serve many other parties—dramatically increasing the potential for security and privacy leaks, in addition to the threats associated with traditional vulnerabilities. This is especially true because once data is opened up outside internal firewalls, many traditional security and privacy approaches do not work (Moura & Serrão, 2016). For example, it becomes much more difficult to monitor and control the flow of data, especially as it goes into third-party hands or crosses national borders, thus involving international law, which may or may not agree with national laws regarding jurisdiction, the nature of the crime, and the 'rights' of victims.

From a privacy perspective, it is now easy to de-anonymise a person using triangulated data from multiple sources (De Montjoye *et al.*, 2015), and data aggregators are doing exactly that. In creating detailed, highly accurate profiles without ever interacting with the person (Davenport *et al.*, 2007), they also create new, ever-challenging security and privacy issues. And it is difficult to stay abreast of them all. For example, how do we enforce encryption of big data that is so massive it is stored in a clustered database across multiple servers, which may not even be geographically collocated? How do we carefully transmit such data without exposing our organisations to great vulnerabilities, when the Internet was not designed for that kind of volume? Up to what point will people stay 'compliant' and agree to have their

data and behaviour gathered and aggregated by organisations and governments throughout the world? More frequently than before, incidents of corporate or government misuse of data get reported in the news. These, along with reports of large information leaks and data breaches, have raised public awareness about the power of data, how personal information is used by businesses and governments, and how often it may fall into the wrong hands. It is possible to expect a change of heart in terms of participation in the global information community, which has been so painstakingly and so diligently built in the name of technological and societal progress.

As is the case with online platforms and the IoT, big data–processing technologies advance faster than the more comprehensive and wholesome chain of systems that preserve information security and privacy (technologies–policies–processes–people–society–economy–legislature), resulting in an increased variety and velocity of vulnerabilities (i.e. the speed at which vulnerabilities appear). Each link of this chain needs the attention of researchers, and thankfully, big data analytics could offer solutions here. For example, big data analytics could be leveraged for the modelling and simulation of resilient supply chains and platforms whose design would limit threat likelihood. Another important contribution of the research in this area is the shaping of organisational and government policies and legislation by identifying baselines and best practices as well as by improving the understanding of human behaviour. As Pentland suggested, 'Companies don't own the data, and that without rules defining who does, consumers will revolt, regulators will swoop down, and the [IoT] will fail to reach its potential' (Berinato, 2014, p. 101). We are already seeing these trends in the European Union (EU), which is introducing challenging legal and social artefacts that are affecting many organisations throughout the world.[7]

[7] The EU's forthcoming General Data Protection Regulation (GDPR) gives more rights back to consumers, streamlines regulations related to international business, and protects customers in the EU *regardless of where the headquarters of the Internet company is located*, and thus will dramatically impact many organisations throughout the world. This regulation goes into effect in May 2018 and has some substantial societal and organisation-level privacy/security implications.

CONCLUSION

In this essay, we outlined some important issues in the hope of moving information security and privacy research forward and enhancing its impact. We discussed the need to re-examine our understanding of IT and IS artefacts and to expand the range of the latter to include those artificial phenomena that are crucial to information security and privacy research. We then briefly discussed and suggested remedies for some common limitations in theory, methodology, and contributions that are bound to weaken a security/privacy study and jeopardise its chances of publication in top IS journals. We illustrated specific improvements that can be made with a couple of in-depth examples that we believe can improve security and privacy research. We challenged the notion of loose re-contextualisation that has gained a foothold in this research area and discussed the example of DT research. We then provided an illustration of how the focus on intentions has undermined the use of powerful theories in security and privacy research, because the theories were designed to capture more than intentions. Finally, we outlined three promising opportunities for IS research that should be particularly compelling to security and privacy researchers: online platforms, the IoT, and big data. All of these carry innate information security and privacy risks and vulnerabilities that can be addressed only by researching each link of the systems chain, that is, technologies–policies–processes–people–society–economy–legislature.

In closing, we introduce the papers in this special issue on security and privacy. Importantly, these were chosen by us and by the *EJIS* editorial team because they demonstrate one or more of the points outlined above and, as such, could make significant contributions to IS security and privacy research.

Moody *et al.* (2017) present a large-scale experimental study that aims to determine the effect of situational and personality factors on individuals' susceptibility to phishing attacks. By explicating underlying theories, the researchers build their model and empirically test it by tracking subjects' actual clicking behaviour. They further explain the likelihood that an individual will fall victim to a phishing attack.

In Posey *et al.* (2017), the authors use advanced data-mining techniques to conduct breach analysis and build a taxonomy of eight major types of personally identifiable information breaches that are currently typical for US organisations. They detail differences in exposure to the breaches and their severity. Like Moody *et al.* (2017), this study has implications for both theory and practice, and it could be used to create a baseline for the different types of attacks across the United States and across organisations.

Cram *et al.* (2017) provide an innovative literature review of studies on organisational information security policies. By reviewing and categorising 76 influential journal articles on security policy, the authors identify core relationships examined in the literature and propose a revised conceptual model that compiles the core construct relationships and provides further theoretical perspectives and insights. This manuscript alone should provide a substantial foundation for future research.

Ozdemir *et al.* (2017) argue that privacy threats have thus far been understood as originating mainly from organisations. Their study challenges this common narrative and instead investigates threats to privacy that result from the misuse of data by social media peers. The authors discuss information privacy and the relevant factors in relation to both institutional and peer contexts and discuss the differences between them in respect of antecedents and consequences.

Algarni *et al.* (2017) investigate social engineering victimisation on social networking sites, Facebook in particular. They analyse users' susceptibility to social engineering victimisation and how it is impacted by the source characteristics on Facebook (such as number of friends, number of posts, common beliefs, good looks, etc.) and source credibility perceptions (such as perceived sincerity, perceived competence, perceived attraction, and perceived worthiness). Such studies of victimisation can help prevent these kinds of abuses in practice.

Finally, Karwatzki et al. (2017) examine the perceived adverse consequences of information disclosure by organisations. Through a focus group study, they develop a categorisation of the consequences of information disclosure and investigate the role of the organisations in each category. As

a contribution to practice, the authors offer mitigation mechanisms with which organisations can address consequences according to category.

Together, our essay and these ground-breaking papers point to a future of compelling research in security and privacy research.

REFERENCES

ACQUISTI A, JOHN LK and LOEWENSTEIN G (2012) The impact of relative standards on the propensity to disclose. *Journal of Marketing Research* 49(2), 160-174.

ALGARNI A, XU Y and CHAN T (2017) An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems* this volume(this issue), TBD.

ALVESSON M and SANDBERG J (2011) Generating research questions through problematization. *Academy of Management Review* 36(2), 247-271.

ANDENAES J (1952) General prevention. Illusion or reality? *Journal of Criminal Law, Criminology, and Police Science* 43(2), 197-198.

ANDERSON BB, VANCE A, KIRWAN CB, EARGLE D and JENKINS JL (2016) How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems* 25(4), 364-390.

ANGST C and AGARWAL R (2009) Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly* 33(2), 339-370.

ANGST CM, BLOCK ES, D'ARCY J and KELLEY K (2017) When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly* 41(3), in press.

ARMSTRONG M (2006) Competition in two- sided markets. *RAND Journal of Economics* 37(3), 668-691.

AUGUST T and TUNCA TI (2008) Let the pirates patch? An economic analysis of network software security patch restrictions. *Information Systems Research* 19(1), 48-70.

BAGOZZI RP, YI Y and PHILLIPS LW (1991) Assessing construct validity in organizational research. *Administrative Science Quarterly* 36(3), 421-458.

BAKOS Y and KATSAMAKAS E (2008) Design and ownership of two-sided networks: Implications for Internet platforms. *Journal of Management Information Systems* 25(2), 171-202.

BANSAL G and GEFEN D (2015) The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems* 24(6), 624-644.

BASKERVILLE R, ROWE F and WOLFF F-C (2017) Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective. *Data Base for Advances in Information Systems* In press(December).

BAUER J, FRANKE N and TUERTSCHER P (2016) Intellectual property norms in online communities: How user-organized intellectual property regulation supports innovation. *Information Systems Research* 27(4), 724-750.

BECCARIA C (2009) On Crimes and Punishments and Other Writings. University of Toronto Press.

BECKER G (1968) Crime and punishment: An economic approach. *Journal of Political Economy* 76(2), 169-217.

BEEGLE LE (2007) Rootkits and their effects on information security. *Information Systems Security* 16(3), 164-176.

BÉLANGER F and CROSSLER R (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35(4), 1017-1041.

BENBASAT I and BARKI H (2007) Quo vadis TAM? *Journal of the Association for Information Systems* 8(4), Article 7.
BENBASAT I and ZMUD RW (2003) The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. *MIS Quarterly* 27(2), 183-194.
BENTHAM J (1988) The Principles of Morals and Legislation. Prometheus Books, Amherst, NY.
BERINATO S (2014) With big data comes big responsibility. *Harvard Business Review* 92(11), 100-104.
BLUMSTEIN A, COHEN J and FARRINGTON D (1988) Criminal career research: Its value for criminology. *Criminology* 26(1), 1-35.
BOSS SR, GALLETTA DF, LOWRY PB, MOODY GD and POLAK P (2015) What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* 39(4), 837-864.
BRANTINGHAM P and BRANTINGHAM P (1991) Environmental Criminology (2nd ed.). (2nd ed.). Waveland Press, Prospect Heights, IL.
BREWER M (2000) Research design and issues of validity. In *Handbook of Research Methods in Social and Personality Psychology* (REIS H and JUDD C, Eds.), Cambridge University Press, Cambridge, UK.
BULGURCU B, CAVUSOGLU H and BENBASAT I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34(3), 523-548.
BURNS AJ, JOHNSON ME and HONEYMAN P (2016) A brief chronology of medical device security. *Communications of the ACM* 59(10), 66-72.
BURNS AJ, POSEY C, COURTNEY JF, ROBERTS TL and NANAYAKKARA P (2017a) Organizational information security as a complex adaptive system: Insights from three agent-based models. *Information Systems Frontiers* 19(3), 509-524.
BURNS AJ, ROBERTS TL, POSEY C and LOWRY PB (2017b) Examining the influence of organisational insiders' psychological capital on information security threat and coping appraisals. *Computers in Human Behavior* 68(March), 190-209.
CALIENDO M, CLEMENT M, PAPIES D and SCHEEL-KOPEINIG S (2012) Research Note—The cost impact of spam filters: Measuring the effect of information system technologies in organizations. *Information Systems Research* 23(3-part-2), 1068-1080.
CAVUSOGLU H, RAGHUNATHAN S and CAVUSOGLU H (2009) Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Information Systems Research* 20(2), 198-217.
CHATTERJEE S and SARKER S (2013) Infusing ethical considerations in knowledge management scholarship: Toward a research agenda. *Journal of the Association for Information Systems* 14(8), 452-481.
CHATTERJEE S, SARKER S and VALACICH JS (2015) The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems* 31(4), 49-87.
CHEN H, CHIANG RH and STOREY VC (2012) Business intelligence and analytics: From big data to big impact. *MIS Quarterly* 36(4), 1165-1188.
CHEN M, JACOB VS, RADHAKRISHNAN S and RYU YU (2015) Can payment-per-click induce improvements in click fraud identification technologies? *Information Systems Research* 26(4), 754-772.
CHEN P-Y, KATARIA G and KRISHNAN R (2011) Correlated failures, diversification, and information security risk management. *MIS Quarterly* 35(2), 397-422.
CHEN Y, RAMAMURTHY K and WEN K-W (2013) Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems* 29(3), 157-188.

CHOI BCF, JIANG ZJ, XIAO B and KIM SS (2015) Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research* 26(4), 675-694.

CLARKE R and CORNISH D (1985) Modelling offender's decisions: A framework for policy and research. In *Crime and Justice: An Annual Review of Research (Vol. 6)* (TONRY M and MORRIS N, Eds.), pp 147-185, University of Chicago Press, Chicago, IL.

CRAM WA, PROUDFOOT JG and D'ARCY J (2017) Organizational information security policies: A review and research framework. *European Journal of Information Systems* forthcoming.

CROSSLER RE, JOHNSTON AC, LOWRY PB, HU Q, WARKENTIN M and BASKERVILLE R (2013) Future directions for behavioral information security research. *Computers & Security* 32(February).

CROSSLER RE, LONG JH, LORAAS TM and TRINKLE BS (2014) Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems* 28(1), 209-226.

CROSSLER RE and POSEY C (2017) Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems* 18(7), 487-515.

CULNAN MJ and WILLIAMS CC (2009) How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly* 33(4), 673-687.

CURRIE W (2009) Contextualising the IT artifact: Towards a wider research agenda for IS using institutional theory. *Information Technology & People* 22(1), 63-77.

D'ARCY J and HERATH T (2011) A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems* 20(6), 643-658.

D'ARCY J, HOVAV A and GALLETTA D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research* 20(1), 79-98.

D'AUBETERRE F, SINGH R and IYER L (2008) Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems* 17(5), 528-542.

D'ARCY J, HERATH T and M. S (2014) Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems* 31(2), 291-325.

DAVENPORT TH, HARRIS JG, JONES GL, LEMON KN, NORTON D and MCCALLISTER MB (2007) The dark side of customer analytics. *Harvard Business Review* 85(5), 37-48.

DAVIS FD, BAGOZZI RP and WARSHAW PR (1989) User acceptance of computer technology: A comparison of two theoretical models. *Management Science* 35(8), 982-1003.

DE MONTJOYE Y-A, RADAELLI L and SINGH VK (2015) Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science* 347(6221), 536-539.

DEY D, LAHIRI A and ZHANG G (2012) Hacker behavior, network effects, and the security software market. *Journal of Management Information Systems* 29(2), 77-108.

DINEV T, GOO J, HU Q and NAM K (2009) User behavior towards protective information technologies: The role of cultural differences between the United States and South Korea. *Information Systems Journal* 19, 391-412.

DINEV T, HU Q and YAYLA A (2008) Is there an online advertisers' dilemma? A study of click fraud in the pay-per-click model. *International Journal of Electronic Commerce* 13(2), 29-59.

DINEV T, MCCONNELL AR and SMITH HJ (2015) Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "Apco" box. *Information Systems Research* 26(4), 639-655.

DINEV T, XU H, SMITH HJ and HART P (2013) Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* 22(3), 295-316.

FELSON M (1994) Crime and Everyday Life: Insight and Implications for Society. Pine Forge Press, Thousand Oaks, CA.
FRENCH AM, GUO C and SHIM JP (2014) Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems* 35, 10.
GARBA AB, ARMAREGO J, MURRAY D and KENWORTHY W (2015) Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information Privacy and Security* 11(1), 38-54.
GEFEN D and PAVLOU P (2012) The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research* 23(3), 940-959.
GERLACH J, WIDJAJA T and BUXMANN P (2015) Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *Journal of Strategic Information Systems* 24(1), 33-43.
GIBBS JP (1975) Crime, Punishment, and Deterrence. Elsevier, New York, NY.
GOEL S, WILLIAMS K and DINCELLI E (2017) Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems* 18(1), 22-44.
GOES P (2013) Information systems research and behavioral economics. *MIS Quarterly* 37(3), iii-viii.
GOODE S, HOEHLE H, VENKATESH V and BROWN SA (2017) User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly* 41(3), 703-727.
GREENAWAY KE, CHAN YE and CROSSLER RE (2015) Company information privacy orientation: A conceptual framework. *Information Systems Journal* 25(6), 579-606.
HAATAJA K and TOIVANEN P (2010) Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures. *IEEE Transactions on Wireless Communications* 9(1).
HAGAN J (1997) Defiance and despair: Subcultural and structural linkages between delinquency and despair in the life course. *Social Forces* 76(1), 119-134.
HAGER CT and MIDKIFF SF (2003) An analysis of Bluetooth security vulnerabilities. In *Wireless Communications and Networking, 2003 (WCNC 2003)*, pp 1825-1831, IEEE.
HARRINGTON SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly* 20(3), 257-278.
HASSAN NR and LOWRY PB (2015) Seeking middle-range theories in information systems research. In *International Conference on Information Systems (ICIS 2015)*, AIS, Fort Worth, TX.
HEIKKILA FM (2007) Encryption: Security considerations for portable media devices. *IEEE Security & Privacy* 5(4).
HERATH T and RAO HR (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47(2), 154-165.
HERATH T and RAO HR (2009b) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18(2), 106-125.
HSU JS-C, SHIH S-P, HUNG YW and LOWRY PB (2015) The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research* 26(2), 282-300.
HU Q, DINEV T, HART P and COOKE D (2012) Top management championship, organizational culture and individual behavior towards information security. *Decision Sciences* 43(4), 615-659.
HU Q, XU ZC, DINEV T and LING H (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM* 54(6), 34-40.
HUI KL, KIM SH and WANG QH (2017) Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly* 41(2), 497-523.
HUI KL, TEO HH and LEE SYT (2007) The value of privacy assurance: An exploratory field experiment. *MIS Quarterly* 31(1), 19-33.
HUTH CL, CHADWICK DW, CLAYCOMB WR and YOU I (2013) Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers* 15(1), 1-4.

JOHNSTON AC and WARKENTIN M (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quarterly* 34(3), 549-566.
JOHNSTON AC, WARKENTIN M, MCBRIDE M and CARTER L (2016) Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems* 25(3), 231-251.
JOHNSTON AC, WARKENTIN M and SIPONEN M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* 39(1), 113-134.
KARAME G (2016) On the security and scalability of Bitcoin's blockchain. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp 1861-1862, ACM.
KARJALAINEN M and SIPONEN M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* 12(8), 518-555.
KARWATZKI S, TRENZ M, TUUNAINEN VK and VEIT D (2017) Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems* this volume(this issue), TBD.
KEITH MJ, BABB J, FURNER CP, ABDULLAT A and LOWRY PB (2016) Limited information and quick decisions: Consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction* 8(3), 88-130.
KEITH MJ, BABB J, LOWRY PB, FURNER CP and ABDULLAT A (2015) The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal* 25(4), 637-667.
KEITH MJ, THOMPSON SC, HALE J, LOWRY PB and GREER C (2013) Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies* 71(12), 1163-1173.
KIM C, TAO W, SHIN N and KIM K-S (2010) An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications* 9(1), 84-95.
KIM W, JEONG O-R, KIM C and SO J (2011) The dark side of the Internet: Attacks, costs and responses. *Information Systems* 36(3), 675-705.
KOKOLAKIS S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64(January), 122-134.
KORDZADEH N and WARREN J (2017) Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment. *Journal of the Association for Information Systems* 18(1), 45-81.
KRISHNAN V and GUPTA S (2001) Appropriateness and impact of platform-based product development. *Management Science* 47(1), 52-68.
KWON J and JOHNSON ME (2014) Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly* 38(2), 451-572.
LAVIN F (2017) Traditional retail might not be dead, but It Is In a coffin. *Forbes*,https://www.forbes.com/sites/franklavin/2017/04/17/traditional-retail-might-not-be-dead-but-it-is-in-a-coffin/#7096e0c549e8, accessed August 31, 2017.
LEE AS (1999) Rigor and relevance in MIS research: Beyond the approach of positivism alone. *MIS Quarterly* 23(1), 29-33.
LEE AS, THOMAS M and BASKERVILLE RL (2015) Going back to basics in design science: From the information technology artifact to the information systems artifact. *Information Systems Journal* 25(1), 5-21.
LEE CH, GENG X and RAGHUNATHAN S (2016) Mandatory standards and organizational information security. *Information Systems Research* 27(1), 70-86.
LEE SM, LEE SG and YOO S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management* 41(6), 707-718.

LEE Y and LARSEN KR (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems* 18(2), 177-187.
LI H, SARATHY R, ZHANG J and LUO X (2014) Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal* 24(6), 479-502.
LI X-B and QIN J (2017) Anonymizing and sharing medical text records. *Information Systems Research* 28(2), 332-352.
LIU CZ, GAL-OR E, KEMERER CF and SMITH MD (2011) Compatibility and proprietary standards: The impact of conversion technologies in IT markets with network effects. *Information Systems Research* 22(1), 188-207.
LOWRY PB, CAO J and EVERARD A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems* 27(4), 163-200.
LOWRY PB, D'ARCY J, HAMMER B and MOODY GD (2016a) 'Cargo Cult' science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *Journal of Strategic Information Systems* 25(3), 232-240.
LOWRY PB and MOODY GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal* 25(5), 433-463.
LOWRY PB, MOODY GD and CHATTERJEE SS (2017a) Using IT design to prevent cyberbullying. *Journal of Management Information Systems* 34(3), in press; doi: http://dx.doi.org/10.1080/07421222.07422017.01373012.
LOWRY PB, MOODY GD, VANCE A, JENSEN ML, JENKINS JL and WELLS T (2012) Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the Association for Information Science and Technology* 63(4), 755-776.
LOWRY PB, POSEY C, BENNETT RJ and ROBERTS TL (2015) Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal* 25(3), 193-230.
LOWRY PB, POSEY C, ROBERTS TL and BENNETT RJ (2014) Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics* 121(3), 385-401.
LOWRY PB, ZHANG J, WANG C and SIPONEN M (2016b) Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model. *Information Systems Research* 27(4), 962-986.
LOWRY PB, ZHANG J and WU T (2017b) Nature or nurture? A meta-analysis of the factors that maximize the prediction of digital piracy by using social cognitive theory as a framework. *Computers in Human Behavior* 68(March), 104-120.
LUO X and LIAO Q (2007) Awareness education as the key to ransomware prevention. *Information Systems Security* 16(4), 195-202.
MARTINSONS MG and MA D (2009) Sub-cultural differences in information ethics across China: Focus on Chinese management generation gaps. *Journal of the Association for Information Systems* 10(11), 816-833.
MENON S and SARKAR S (2016) Privacy and big data: Scalable approaches to sanitize large transactional databases for sharing. *MIS Quarterly* 40(4), 963-981.
MERHOUT JW and HAVELKA D (2008) Information technology auditing: A value-added IT governance partnership between IT management and audit. *Communications of the Association for Information Systems* 23(1), 26.

MILTGEN C and SMITH HJ (2015) Exploring information privacy regulation, risks, trust, and behavior. *Information & Management* 52(6), 741-759.
MINGERS J and WALSHAM G (2010) Toward ethical information systems: The contribution of discourse ethics. *MIS Quarterly* 34(4), 833-854.
MOODY GD, GALLETTA DF and DUNN BK (2017) Which phish get caught? An exploratory study of individuals' susceptibility to phishing. *European Journal of Information Systems* this volume(this issue), TBD.
MOURA J and SERRÃO C (2016) Security and privacy issues of big data. *Working paper* preprint.
MYYRY L, SIPONEN M, PAHNILA S, VARTIAINEN T and VANCE A (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* 18(2), 126-139.
NIEMIMAA E and NIEMIMAA M (2017) Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems* 26(1), 1-20.
OETZEL MC and SPIEKERMANN S (2014) A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems* 23(2), 126-150.
ORLIKOWSKI WJ and IACONO CS (2001) Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information Systems Research* 12(2), 121-134.
OZDEMIR ZD, SMITH HJ and BENAMATI JH (2017) Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems* this volume(this issue), TBD.
PAQUETTE S, JAEGER PT and WILSON SC (2010) Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 27(3), 245-253.
PARKER G, ALSTYNE MV and JIANG X (2017) Platform ecosystems: How developers invert the firm. *MIS Quarterly* 41(1), 255-266.
PARKS R, XU H, CHU CH and LOWRY PB (2017) Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems* 26(1), 37-65.
PAVLOU P (2011) State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly* 35(4), 977-988.
PEACE AG, GALLETTA DF and THONG JYL (2003) Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems* 20(1), 153-177.
POSEY C, BENNETT RJ, ROBERTS TL and LOWRY PB (2011) When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security* 7(1), 24-47.
POSEY C, LOWRY PB, ROBERTS TL and ELLIS S (2010) Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems* 19(2), 181-195.
POSEY C, RAJA U, CROSSLER RE and BURNS AJ (2017) Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems* this volume(this issue), TBD.
POSEY C, ROBERTS TL and LOWRY PB (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* 32(4), 179-214.
POSEY C, ROBERTS TL, LOWRY PB, BENNETT RJ and COURTNEY J (2013) Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly* 37(4), 1189-1210.
POSEY C, ROBERTS TL, LOWRY PB and HIGHTOWER R (2014) Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management* 51(5), 551-567.
PRIES-HEJE J and BASKERVILLE R (2008) The design theory nexus. *MIS Quarterly* 32(4), 731-755.

RAI A (2017) Avoiding type III errors: Formulating IS research problems that matter. *MIS Quarterly* 41(2), iii-vii.
RANSBOTHAM S and MITRA S (2009) Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research* 20(1), 121-139.
ROCHET JC and TIROLE J (2006) Two- sided markets: A progress report. *RAND Journal of Economics* 37(3), 645-667.
SAMPSON R and LAUB J (2005) A life-course view of the development of crime. *The Annals of the American Academy of Political and Social Science* 602(1), 12-45.
SIMON HA (1996) The Sciences of the Artificial. MIT Press, Boston, MA.
SINGH J, PASQUIER T, BACON J, KO H and EYERS D (2015) Twenty cloud security considerations for supporting the Internet of Things. *IEEE Internet of Things Journal* 3(3), 269-284.
SIPONEN M, PAHNILA S and MAHMOOD A (2007) Employees' adherence to information security policies: An empirical study. In *New Approaches for Security, Privacy and Trust in Complex Environments* pp 133-144, Springer.
SIPONEN M and VANCE A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3), 487-502.
SIPONEN M and WILLISON R (2009) Information security management standards: Problems and solutions. *Information & Management* 46(5), 267-270.
SMITH HJ, DINEV T and XU H (2011) The information privacy research: An interdisciplinary review. *MIS Quarterly* 35(4), 989-1016.
SON J-Y (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management* 48(7), 296-302.
SONG P, XUE L, RAI A and ZHANG C (2017) The ecosystem of software platform: A study of asymmetric cross-side network effects and platform governance. *MIS Quarterly* forthcoming.
SPEARS JL and BARKI H (2010) User participation in information systems security risk management. *MIS Quarterly* 34(3), 503-522.
STRAUB DW (1990) Effective IS security. *Information Systems Research* 1(3), 255-276.
SUBASHINI S and KAVITHA V (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1), 1-11.
SUMNER M (2009) Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management* 26(1), 2-12.
TANG Z, HU YJ and SMITH MD (2008) Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems* 24(4), 153-173.
TE'ENI D, ROWE F, ÅGERFALK PJ and LEE JS (2015) Publishing and getting published in EJIS: Marshaling contributions for a diversity of genres. *European Journal of Information Systems* 24(6), 559-568.
TSAI J, EGELMAN S, CRANOR L and ACQUISTI A (2011) The effect of online privacy information on purchasing behavior: An experiment study. *Information Systems Research* 22(2), 254-268.
TSIAKIS T and STHEPHANIDES G (2005) The concept of security and trust in electronic payments. *Computers & Security* 24(1), 10-15.
TSOHOU A, KARYDA M, KOKOLAKIS S and KIOUNTOUZIS E (2015) Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems* 24(1), 38-58.
TUREL O and BART C (2014) Board-level IT governance and organizational performance. *European Journal of Information Systems* 23(2), 223-239.
UNDERWOOD S (2016) Blockchain beyond bitcoin. *Communications of the ACM* 59(11), 15-17.
VAN DE VEN AH (2007) Engaged Scholarship: A Guide for Organizational and Social Research. Oxford University Press, New York.

VANCE A, BENJAMIN LOWRY P and EGGETT D (2015) Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly* 39(2).
VANCE A, LOWRY PB and WILSON D (2017) Using trust and anonymity to expand the use of anonymizing systems that improve security across organizations and nations. *Security Journal* 30(3), 979-999.
VEIGA AD and ELOFF JH (2007) An information security governance framework. *Information Systems Management* 24(4), 361-372.
WALL JD, LOWRY PB and BARLOW J (2016) Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems* 17(1), 39-76.
WANG J, GUPTA M and RAO HR (2015a) Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly* 39(1), 91-112.
WANG J, LI Y and RAO HR (2016) Overconfidence in phishing email detection. *Journal of the Association for Information Systems* 17(11), 759-783.
WANG J, LI Y and RAO HR (2017) Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research* 28(2), 378-396.
WANG J, XIAO N and RAO HR (2015b) An exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research* 26(3), 619-633.
WARKENTIN M, JOHNSTON AC, WALDEN E and STRAUB DW (2016) Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems* 17(3), 194-215.
WARKENTIN M and WILLISON R (2009) Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems* 18(2), 101-105.
WHETTEN D, FELIN T and KING B (2009) The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management* 35(3), 537-563.
WHINSTON AB and GENG X (2004) Operationalizing the essential role of the information technology artifact in information systems research: Gray area, pitfalls, and the importance of strategic ambiguity. *MIS Quarterly* 28(2), 149-159.
WILLISON R and WARKENTIN M (2013) Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly* 37(1), 1-20.
WILLISON R, WARKENTIN M and JOHNSTON AC (2017) Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal* forthcoming(doi: 10.1111/isj.12129).
WORKMAN M (2007) Gaining access with social engineering: An empirical study of the threat. *Information Systems Security* 16(6), 315-331.
WRIGHT RT, JENSEN ML, THATCHER JB, DINGER M and MARETT K (2014) Research Note—Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research* 25(2), 385-400.
XU H, TEO HH, TAN BCY and AGARWAL R (2010) The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems* 26(3), 137-176.
ZAHEDI FM, ABBASI A and CHEN Y (2015) Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems* 16(6), 448-484.

ACKNOWLEDGEMENTS

This editorial was circulated among the senior EJIS editorial community and several security and privacy experts. We greatly appreciate their useful feedback. Of those who provided non-anonymous feedback, we would like to thank especially, in alphabetical order, A. J. Burns, Dan Choi, Robert Crossler, John D'Arcy, Dennis Galletta, Allen C. Johnston, Gregory D. Moody, Clay Posey, H. R. Rao, Tom L. Roberts, Frantz Rowe, H. Jeff Smith, Dov Te'eni, and Virpi Kristina Tuunainen.