JeDEM 3(2): 192-206, 2011
ISSN 2075-9517
http://www.jedem.org

Internal Security Institutions Meeting Internet Governance

A Comparative View on the UK and Germany

Mathias Bug*, Jasmin Röllgen**

**Mathias Bug, Researcher, Universität der Bundeswehr München, Institut Politikwissenschaft, mathias.bug@unibw.de, +49 (0)89 6004 2409;*

***Jasmin Röllgen, Researcher, Universität der Bundeswehr München, Institut Politikwissenschaft, jasmin.roellgen@unibw.de, +49 (0)89 6004 4532*

Abstract: *Because of the Internet's ever increasing capacity to offer an infrastructure of open interaction, governmental interest in monitoring the Internet is also growing around the world. A demonstrative example might be the attempts to make any technology-based communication 'traceable' with the help of a European scheme of data retention (EU direction 2006/24/EC) and its national ratifications. Considering this, two assumptions arise: Firstly, governments try to achieve their logic of 'real life' internal security within the realm of the Internet. Secondly, the Internet has changed societies in so far as it has opened space for new relevant communities and actors, who use more and more institutionalised paths of policy shaping. This will be shown by analysing the interaction of institutions and actors involved in the process of data retention implementation in the UK and Germany. Societal and political differences will be briefly touched, as they build the framework of any political decision making process.*

Keywords: Internal Security, Net Policy, Governance, Institutions, Data Retention, Comparative Case Study, UK, Germany

1. Introduction: Internal Security in the Cyber[1]

Germany and the United Kingdom (UK) show similarities in their approaches to internal security. In both countries, the way towards a preventative definition of internal security was paved even before 9/11. Furthermore, in the wake of 9/11, a centralisation of competences favouring the executives has taken place in this policy field as well.

Meanwhile, both societies have entered a knowledge-based era where information and communication technologies (ICT) affect the economy, social life, national and international systems, and the control of crucial infrastructures. Work and life become increasingly intertwined, as borders of privacy become unclear. As well as bringing about tremendous social change, the Internet has also become a potential source of security threats. This is caused by two connected aspects: the mentioned dependency of communication as well as the functioning of crucial infrastructure upon the comparatively insecure Internet on the one hand, together with a growing number of malicious actors with high Internet-competence on the other hand (Dunn Cavelty 2007, p.16). This endangerment of the Internet as a critical infrastructure is nowadays considered a significant hazard.

To some actors, one answer to these threats seems to be a heightened policing of ICTs. In this context, data retention is a hotly discussed measure in Germany and to a lesser extent also in the UK. As will be shown, the measure was introduced already ten years ago; the coverage of Internet traffic however was only taken up in 2009. Therefore, data retention covers any technology-based communication. Considering this example with other security tactics, we will question why the parallel approaches of the two nations' internal security bring about divergent 'successes' and degrees of the

[1] We thank our anonymous reviewers for their explanatory notes.

measures' implementation. By examining this, we hope to clarify what effect the attempt of transferring internal security modes upon the Internet can have on (state) actors and institutions.

Our assumption regarding both of these questions is that the state actors attempt to transfer their conception of traditional internal security into the sphere of the Internet, whilst ignoring the state's dependency on private stakeholders to actually implement its regulation (Zürn/Mayer 2006, p. 473). To understand the resulting conflict, it is important to discover the underlying rationales of the two regimes involved – state dominated internal security politics and its compatibility to Internet governance without much state power (so far). To illustrate this, institutional settings in the framing of internal security policies are described in the next section. Using the regulation of data retention as a case study, we will show how traditional approaches to internal security have been applied to the Internet with mixed results. This will be done in a comparative way; by analysing institutional and actor settings in the UK and Germany, differences in the handling of data retention can be elucidated.

As traditional core-European Union members and important economic players, both countries have a strong influence on European policy making in general. In particular, both countries play crucial roles in internal security policy making on the European level. However, they diverge on important aspects regarding the described research field: they have a different number and institutionalisation of vetoplayers, as well as a different formal and informal influence of private, collective and individual stakeholders. Via a rudimentary policy analysis it will be shown that these differences indicate how state and non-state actors have actually succeeded in shaping the each nation's approach to data retention. On a European level, the UK and Germany actually lie at opposite poles, with the German constitutional court being cited Europe-wide by national constitutional courts (Schweda 2011, p.67) and the UK being a frontrunner in a wide definition and tough implementation of the EC-directive (Beck 2011, p. 104).

2. Veto or No Veto? Prepositions on Internal Security in the UK and in Germany

The difference in scope of security measures can be partly explained by the differences in the two countries' institutional configuration and its central actors. By doing so it is important to describe both institutions and actors in the policy field of internal security. This chapter aims to show institutional differences in the UK and Germany, whilst simultaneously attempting to demonstrate parallel developments regarding internal security policies.

Arguments for tightening security legislation and for security oriented net-regulation in the UK and in Germany need to be seen in the context of long-term developments in the broader policy field, for example their experiences with terrorism, namely the *Rote Armee Fraktion* (RAF) in Germany (until the mid 1990s) and the Northern Irish troubles, which lasted at least until the 1998 Good Friday Agreement and are comparable to a civil war with terrorist actions (Glaeßner 2005, p. 91). Consequently, since 1973, the UK has had strong anti-terrorist policies, even before 9/11 and the London terrorist attacks of 2005 (Büsching 2009, p. 146).

Glaeßner compares the situation of legal activities concerning Northern Irish troubles to the reactions to 9/11. From his point of view, in both cases, the legal thresholds were insufficient to actually protect individual rights (Glaeßner 2005, p. 105). Shortly before the 2005 attacks in London, the UK had begun to be aware of its issues with organised crime, the nature of which is more international than in continental Europe (Glaeßner 2005, p. 86). This perhaps explains why some UK politicians see strong analogies between organised crime and international terrorism (Home Office 2004, p. 1). However, the assumption remains that it is actually the security agencies striving for more power and financial resources. This is done by, for example, defining terrorism in a comparatively wide

manner (Glaeßner 2005, p. 97). The result is wide surveillance of the populace in both public and private spaces (Sturm 2009, S. 204). This doesn't apply to the same extent to Germany.

Despite the harmonising international and European influence through the Council of Europe and the European Union (EU), internal security measures appear more expansive in the UK. However, this picture becomes a little blurry when considering the German socio-historical data collection politics such as compulsory residence registration and its continuously updated filing.

2.1. European Harmony Orchestra

The commonly shared[2] institutional influx on internal security policies in the UK and Germany is highly influenced by the European Union. The European integration process increasingly allows former domestic policies to be discussed and regulated on a European level. For example, not only the threats of terrorism and organised crime, but also questions of policing the Internet or personal data protection have already found EU responses. This is a logical consequence of the relative smallness of European states, making any (security-oriented) Internet regulation being regarded as obsolete if it is not valid for the entire European Union. Already in 2000, the Council of Europe – covering even more nations than the EU – established a convention on Cybercrime which attempted to harmonise policing measures of the Internet (Council of Europe 2001).

However, the European Union is not a parliamentary system of government; therefore the evident 'Europeanisation' of internal security does not mean a Europeanisation of parliamentary control – neither on a European level nor on a national level. Security policy on the European level is still facilitated by national governments. In questions of security, the legal process through the Parliament of the EU is often very streamlined, barely allowing for proper parliamentary checks. The high-level group on the future of European Home Affairs policy is another example of the dominance of governments (Future Group 2008). It consisted of the EU member states' Ministers of Home Affairs and the Commissioner of Home Affairs. The propositions from 2008 were recently redressed as an 'EU Internal Security Strategy' by Commissioner Cecilia Malmström (Malmström 2011). However, the Lisbon Treaty strengthens the European Parliament in matters of internal security. Within the next two years, the consequences of heightened parliamentary influence should become more evident.

Even though there is a high EU influence upon internal securities, the national implementations of EU regulation are not always consistent, as the example of data retention in chapter four will show. A similar situation can be observed in the case of EU-sponsored linkages of national security agents through Europol and Eurojust, whereby not all member states actively take part and provide the required information.

The ambiguities mentioned above are also visible in the EU's influence upon Germany and the UK. National differences in institutions and actor constellations reflect a significant impact upon the national implementation of EU regulation. These differences might be caused by veto players and veto points that are based on questions of government formation, party policy and system, state polity, opposition formation and lobbyism.

Furthermore, internal security is a policy field consisting of fragmented areas such as crime prevention, migration, policing, judicial policy, and also, increasingly in the last decade, Internet policing. The result is also a horizontal sharing of competencies between – for the most part – the Ministries of Justice and Ministries of Internal Affairs. The discussion about data retention is kept up by exactly those ministries on the German *Länder* and federal level. However, the critical stances are especially kept up by faction's speakers for net policy/media and net affine NGOs. The UK shows a

[2] Difference of this influx can be seen in the British non-membership of the Schengen agreement. As we are not focusing on the area of migration and border control, one can speak of a similar influence by the EU regarding internal security.

similar picture. In consequence, it is difficult to define a broader policy field where data retention fits into. In both countries we find an executive superiority in the decision making and implementation of data retention. Hence, we will continue with a description of the policy field of internal security – as this is needed to understand the dynamics of the arguments.[3]

2.2. Multilevel policy making in Germany

While issues around internal security are located on the European and on the national level as mentioned above, there is a further vertical competence sharing within the national level itself. In the German case, the wide ranging *Länder*competence over internal security, especially in the form of the individual *Länder*-police and intelligence forces (there are some 40 different police forces in Germany), is the most obvious expression of this multilevel aspect. Consequently, Germany's federal system and the horizontal and vertical connection between institutions and actors plays an important role in analysing measures of internal security (Frevel/Groß 2008, p. 67). The coordination of the partly heterogeneous internal security policy of the German *Länder* takes place in the *Innenministerkonferenz* (IMK). The IMK is *the* central institution for coordination and (pre-)decision-making in the field of internal security, on both the regional level as well as the federal level. The IMK only makes unanimous and legally non-binding decisions, meaning that once a decision is made, the *Länder*parliaments (if the decisions aren't implemented via decree, leaving the parliaments unconsulted) should find it hard not to set them into law, as the decisions are already the result of rigorous inter-*Länder* compromise.

Furthermore, despite only being a guest, the Federal Minister of the Interior plays an important role in the IMK. Traditionally, his speech opens up the Conference, while presenting the conclusion of the meeting together with the chairman of the IMK closes it. These aspects illustrate two things: the dominance of the executives in internal security matters at the national and *Länder*-levels, and the influence of the federal level on regional policy concerns. One consequence of the policy coordination is the disempowerment of the (*Länder-)*parliaments, as well as the fact that the attribution of policies to actors becomes unclear and non-transparent. Accordingly, (*Länder*-)governments often try to accomplish unpopular decisions by referring them to other pre-deciding policy arenas like the IMK, or to arenas on the European level such as the aforementioned Future Group (Frevel/Groß 2008, pp. 82, 83).

On the German federal level, Governments are coalitions. Governmental strategies regarding internal security are therefore always a compromise between parties, usually between social democrats (SPD) or conservatives (CDU/CSU) and a 'small' coalition partner, such as the Greens (*Bündnis 90/Die Grünen*), the socialists (*Die Linke*) or the liberal democrats (FDP). One commonality between the smaller parties is often a critical stance towards security measures. 'Grand coalitions' between social democrats and conservatives currently exist in only four *Länder,* and there is only one single-party government (up until 2009 one could be found in Bavaria; today there is one in Hamburg). Nevertheless, the *Innenministerkonferenz* shows that there has been something resembling a nationwide grand coalition of internal security in Germany for quite some time (Kutscha 1998, Bukow 2011 p. 29). Remarkably, there is currently no Minister of Internal Affairs in any *Land* stemming from a small party, despite there being eleven *Landes*coalitions with small party participation at present.[4]

In the late 1990s and early 2000s, the German debate on internal security centred around Germany's reunion and the planned European enlargement (Lange 1999, p. 412; Prätorius 2000, p. 381). When looking at the 1998 coalition agreement, the anxiety about expected changes in organised

[3] More about this problem: Bukow 2011, pp. 23-24.

[4] For an overview, see: http://www.bundesrat.de/cln_179/nn_8780/DE/gremien-konf/fachministerkonf/imk/Vorsitz-und-Mitglieder/uebersicht-node.html?__nnn=true. Checked on 3.5.2011

and white-collar crime becomes immediately evident (SPD/Bündnis 90/Die Grünen 1998, p. 37). Political and religious terrorism, on the other hand, had barely been a concern (anymore) until September 11th 2001.[5] In reaction to 9/11, German law makers passed the so-called Security Packages I and II in an astoundingly short period, ostensibly in order to facilitate law enforcement against terrorist attacks. The UK's ATCSA was passed in similar haste (Whitley/Hosein 2005, p. 863).

When looking at parties engaging in internal security, it is worth noting that internal security is not traditionally a 'conservative' field. In Germany, it is the CDU/CSU as well as SPD who seem to be striving to push security legislation in the same direction. Already in 1980, it could be seen that Social Democratic policymaking on internal security was even more restrictive than that of conservative parties. Arguably, this is because SPD governments have seen themselves as 'put on the spot' by accusations of having a problem-solving deficit regarding security (Schmidt 1980, pp.192-193).[6]

It is therefore not surprising that the German second chamber, the *Bundesrat*, does not play a veto role in strengthening security measures that need to be confirmed in the *Bundesrat* – despite the existence of small party participation coalitions in the *Länder*. However, as the example of data retention will show, it is actually the second chamber and the IMK who have been lobbying for it since 2000. (Spittmann 2000, Bukow 2011, p. 39). Furthermore, the *Bundesverfassungsgericht* has played an important role as the central veto player in the legislative process regarding security issues. Bukow suggests this is a logical consequence of the court's competence of demarcation between freedom and security (Bukow 2009, p. 354). Taking it further, Hornung and Schnabel see systematic changes in the legislative process. They have based their findings on experience stemming from three different *Bundesverfassungsgerichts*-decisions, namely the online searching of computers, automatic license plate recognition, and data retention. In general, they criticize the relative careless implementation (in regard to constitutional rights), and consequently view an integration of judicial checks into the policy process in internal security as follows:

> *"[…] the scrapping rulings of the Bundesverfassungsgericht are then used like expert opinions to see which safeguards are absolutely necessary to avoid the enabling act from being annulled again." (Hornung/Schnabel 2009, p. 122)*

2.3. Developments in UK policy making – Devolution and Coalition

This hastening of the securitisation of policy processes seems to apply to the UK and its Labour government over the last decade as well (Whitley/Hosein 2005, p. 863). Consequently, the in 2010 elected coalition in London wrote in its coalition agreement:

> *"The Government believes that the British state has become too authoritarian, and that over the past decade it has abused and eroded fundamental human freedoms and historic civil liberties. We need to restore the rights of individuals in the face of encroaching state power, in keeping with Britain's tradition of freedom and fairness." (Government 2010, p.11)*

This quote also hints that vertical competence sharing within the UK plays a minor role. However, there is no unitary British policymaking in this area either. 'British internal security policy' mostly refers to England and in the majority of cases to Wales. Northern Ireland and Scotland generally have specifications in security Acts and a distinctive legal basis.[7] These heterogeneities are the result of asymmetric devolution. However, competencies of the Scottish and Northern Irish parliaments are restricted to their own region. Before the Welsh referendum, it had no primary legislative competence

[5] At least since the self-liquidation of the RAF in 1998, terrorism had been alleviated from the national political consciousness. But in reality there had been no physical manifestation of terrorism since the last RAF terrorist attack in 1993

[6] For a current but similar argument see: Kunz 2004, pp. 16-17. The Britisch Labour party – arguably – has to struggle with the same constellation.

[7] See for example: Terrorism Act 2000.

like Scotland or Northern Ireland; the National Assembly for Wales simply had a right to be heard by Westminster Parliament (Sydow 2005, p. 62). Increasingly, there is a trend toward further devolution, but there cannot be said to be a multilevel character of inner security as such, chiefly because the agenda-setting power remains in London (Bug et al. 2011, p. 56).

Up until recently, single party Governments have been the central actors in the UK regarding inner security. Even the British history of decentralised, community-oriented policing cannot levy the government's role, especially after the structural reforms centralising policing contained in the 2004 'One Step Ahead' strategy paper (Glaeßner 2005, p. 95). This, however, puts even more power into the hands of the mostly single-party government in London.

However, as one can already see in recent governmental papers, even further measures such as data retention of social network content have been carried over from Brown government policies into the recent Strategic Defence and Security Review contradicting the new coalition agreement. (Williams 2010) – arguably, this seems to be logical when regarding Castells argument that control of information is state power and therefore state sovereignty (Castells 2005, p. 191).

Even though the Liberal Democrats' influence on further security legislation has remained moderate, the landmark of the first coalition government since World War II is noteworthy and might lead to central institutional changes, especially concerning the role of parliament and parties in general. So far, opposition to security measures has been more a question of chambers than of party membership. Looking at the anti-terrorism legislation since 9/11, the legislative processes were comparatively swift in the House of Commons, whereas it was the House of Lords reaching for less incisive rules (Sturm 2009, p. 130). This observation is supported by Whitley and Hosein with the focus on information based communication regulation; they give the Regulation of Investigatory Powers Act 2000 as an early example (Whitley/Hosein 2005, p. 862).

Furthermore, the Lord's Appeleate Committee, the highest level of jurisdiction (in 2009 it was turned into the Supreme Court) was recruited from the House of Lords. For instance, it played a restraining role in the discussion about security measures in the ATCSA.

3. Black Box Internet Governance

In general, issues about the protection of citizens against malicious actors, whether internal or extrernal, are usually tackled with approaches to governing and managing security with regard to a specific territory. However, if state actors also wish to protect their inhabitants from so-called 'cyber threats', they need to take into account that the Internet as an infrastructure and the control of its content works with different actors and institutions compared to physical space and interaction. As Dunn Cavelty indicates, far more public-private and national-international cooperation is needed, as well as more societal engagement (Dunn Cavelty 2011, p. 58). Mathiason sees the power relation as follows:

> *"The Internet's pervasiveness is changing politics, economics and social relations. Its borderless nature affects the roles of individuals, the magic of the marketplace and the problems of government regulation. […] the Internet is a field where the private sector and civil society each have a role as important - or sometimes more important - than governments." (Mathiason 2009, p. 2)*

Traditional open space is restricted by national borders wherein legal institutions structure the policies which elected representatives make. It is obviously spatially located. On the contrary, the Internet is global, non-territorial and transcends notions of 'nationhood'. Nevertheless, from a democratic perspective, the coordinating part of regulation should remain with the governments as the legal centres of regulation (Shahin 2007, p. 13). On the other hand, private actors offer technology to

offset both regulative measures implemented by states or attacks initiated by criminals or states (i.e. by anonymizing, encryption).

However, it is also the conception of security that seems to make a difference:

> *"In national security, security is a binary concept: either one is secure or one is insecure. By contrast, computer security or information assurance is concerned with analysing the risk to information networks of all sorts and then mitigating the identified risks by technical (and occasionally organisational) means." (Dunn Cavelty 2011, p. 59)*

It is questionable in times of asymmetric threats and climate change whether national security is actually binary. However, in public statements, it might often appear as if this is the case. We argue that the state actors in the field of internal security in Germany and the UK attempt to transfer this binary conception of traditional internal security to the sphere of the Internet and that a risk discourse – parallel to classical internal security – is barely taking place.

If state actors try to regulate or control Internet activity, or if Internet activists or the copyright industry try to shape the policy making process, the inherently different logics of the two spheres become problematic. The fear or hope for the latter two groups is that alleged security measures could easily build the technological foundation for measures aiming to satisfy further interests. This becomes most obvious when considering that states might have to integrate economic interests (for instance of the copyright industry) into their decision making. In that case, retained connection data would become accessible to copyright cases and would not only be accessible for heavy crime. The intensity of the resulting competition for power would decide the success and design of internal security measures regarding the Internet. To understand the critical juncture in this case, we will need to briefly describe the perspectives of both sides and why they sit uncomfortably together. We will focus on the security arguments, as the wider context cannot be adequately addressed in this context.

3.1. Physical and Virtual Open Space

The distinctiveness of the spheres of traditional policymaking in a specific territorial area and the Internet – which is not territorial and barely physically restricted – makes it difficult for political actors to capture and handle internal security threats regarding the Internet. This raises general problems around law enforcement. It requires clear localisation to know firstly which legislation applies, and secondly to whom it has to be applied (i.e. who is the criminal?). Those questions, in general, can be solved (Brodowski/Freiling 2011, p. 164). However, technologically savvy or cautious users often evade detection, given that the Internet a poorly traceable interface. As a result, there are often attempts to make the Internet more traceable, such as the recent calls for less anonymous social networks and data retention.

This raises the question of whether state actors should extend their regulation and law enforcement concepts into cyberspace as well. In the virtual sphere, one cannot simply regulate specific fields. Regulation always has an effect on activity across the entire Internet, including privacy and personal rights. Therefore, one could argue, a reduction of personal rights is the price of a policeable Internet. As a result, it appears that state actors in domestic policy have vastly different priorities and see different issues in terms of personal rights and internal security than actors within the Internet community. It is the challenge of state actors to balance their citizens' internal and external security with their personal rights. But there is a general problem in securing these rights: it is possible that security threats are planned or implemented within the Internet, but it is not possible to regulate the Internet in the same way as traditional open space. Furthermore, it is possible that personal rights are violated twofold – via the Internet as well as by lawmakers through Internet regulation mechanisms. Hence more cooperation is needed and state actors might need restore some faith in public-private

cooperations, as for example the successful fight against child pornography online shows (Brodowski 2011, p. 156). This explains the recent Internet community's broadening focus on state and Internet services (such as social networks etc.) as a violator itself (quite prominently e.g. Kurz/Rieger 2011).

On a European as well as a national level, there are several salient regulating examples, including the *Jugendmedienstaatsvertrag*, the *Glücksspielstaatsvertrag* and the *Zugangserschwerungsgesetz* in Germany or recent calls to better cooperate in monitoring the telecommunication in the EU (Krempl/ Haupt 2011) and to create a "single secure European cyberspace" in order to "block illicit contents on the basis of the EU 'black-list'" (Council of the European Union, 2011, p. 4), a result of the joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party. These approaches show the state's effort to control the virtual space by giving it territorial, national and supranational, or content-related borders. All the examples were highly criticised for their censoring effect and potential for misuse.

3.2. Hierarchy and polycentrism

Although there are multilevel aspects regarding this policy field, internal security is organised centrally and according to hierarchy in each region. The policymaking and execution of security measures is obviously structured in such a way that competences and responsibilities should be clear. This does not mean that the policymaking process in internal security is a closed circle, not open to influence from practitioners, experts, scientists or the information and communication industries. Nonetheless, their ability to shape policies is restricted as long as the final decision makers remain elected state actors and the policy field continues to be formally regulated from the top down. Regarding policymaking in the realm of the Internet, Mathiason contends that

> *"While it might seem that governments should run the Internet, in reality there are five groups of stakeholders in governance, and the debate on governance turns on the role for each. The five are: 1 Individual governments reflecting national interests; 2 International organizations, reflecting the views of their inter-governmental bodies and their secretariats; 3 The private sector, consisting of corporations - mostly multinational - working as individuals or through their associations such as the International Chamber of Commerce; 4 Non-governmental organizations, […] 5 Academics […]" (Mathiason 2009, pp. 19, 23)*

However, it still needs to be stated that these groups and their proclaimed interests are not homogenous and are partly interlinked. The example of data retention will show Mathiason's five groups' dividedness. It occurs because of interest formation, articulation and group building. In short: interaction via the internet is not clearly structured hierarchically with one or a few dominant and governing actors. Rather, it is polycentric and horizontal. The accumulation and verbalisation of interests or strategies does not work towards one centre. Moreover, it is hardly possible to talk about 'the' Internet community: there are many different groups in multiple spheres such as work, social life, or privacy, and none of these takes precedence as the most important or influential – as was shown above with the example of privacy rights interests versus copyright industries.

Nevertheless, each of the actor-groups Mathiason named above, especially group 4 and 5, has become increasingly integrated into political institutions in the last decade. Especially groups 4 and 5 are partially interlinked and also show some connection to parliamentarians from small or opposition parties – mostly from the Green Party in Germany. This relation was not mentioned by Mathiason. They are poorly financed (compared to industry lobbyism) and dependent on individual representatives/speakers. Nonetheless, their institutionalisation could be measured by their

participation in parliament hearings[8] or statements to courts, as will be shown in the next chapter. However, in the German case, it should be noted that so far the prominent NGOs such as FoeBuD and the Chaos Computer Club do not seem to place emphasis on the federal aspect of internal security in their lobbyism, as their important individual representatives tend to work prominently in and from Berlin (Wendelin/Löblich 2011, p.3).

4. Data Retention – Making the Internet and its Actors Traceable

Data retention is arguably the most prominent surveillance measure implemented in the area of information and communication technologies. This might also be caused by the fact that the measure affects everybody using any kind of telecommunication. However, the issue of data retention was especially discussed around the technology of the Internet. In the wake of 9/11, the Internet became increasingly perceived as a 'meeting place for terrorists'. In this chapter we will try to describe the development of data retention from the early British steps over the EC-directive up to the implementations of the directive. We will aim to place an emphasis on the scope and consequences of data retention, as well as on the different actors involved in the decision making processes in the UK and Germany.

The UK introduced a policy of data retention covering every British phone user as early as 2001 in the UK Anti Terrorism Crime and Security Bill (ATCSA), technically based on the Regulation of Investigatory Powers Act (RIPA) from 2000 (Whitley/Hosein 2005, p. 864). Despite the wide accessibility granted by RIPA, the ATCSA was presented to parliament exclusively as a measure to combat terrorism[9] (Whitley/Hosein 2005, p. 863). The ATCSA worked on a voluntary level focusing on the big communications services providers. Furthermore, it used different retention periods depending on the types of data. Keeping the role of the industry in the communications sector in mind (Whitley und Hosein 2005, S. 858), the regulations were discussed with providers and individual ways of reimbursing them were found, which didn't make the process any more transparent (Walker 2009, p. 326).

After the attacks in Madrid (2004) and London (2005), a European solution to data retention became feasible – and was swiftly introduced. Walker describes the development as follows:

> *"In the wake of the Madrid bombings in March 2004, the UK and three other Member States tabled a controversial draft Framework Decision proposing retention periods of one to three years. Those plans were rejected by the European Parliament on 7 June 2005, with the European Commission hinting at an alternative approach by means of a directive. Exactly one month later, however, the London bombings of 7 July put the Framework Decision back on the agenda of the European Council, under a UK Presidency." (Walker 2009, p. 326)*

Consequently, the UK regulation changed partly after the Directive 2006/24/EC was set into force in the UK in 2007, and included Internet data in 2009. The respective regulations made data retention mandatory for informed communications providers, and the retention time was set for all data to twelve months (Home Office 2009, p. 10). To avoid the double-up of saved data, providers only fall subject to mandatory retention if they are informed by the government. Furthermore, the reimbursements remain as individual agreements between providers and the government. These two aspects mirror the emphasis the UK government put on the acceptance of providers in the implementation process of the directive. This was also illustrated by the design of the Home Office's consultation: "The consultation questions are primarily aimed at communications service providers and the implications that

[8] In the German case, the factions invite specialists who are mostly representatives for specific interests, whereas in Britain participation in the consultation process of bills is open to everyone.

[9] Even though there is little evidence of success in regard to fighting terrorism by the means of data retention (Krempl/Meyer 2010).

implementation of the directive will have on them." (Crossman/Liberty 2008) This view from Liberty, one of the main British NGOs for civil liberties and human rights, is confirmed by the following quote from the Home office's Response from the consultation process, which shows how little the NGOs from civil society were taken seriously:

> *"The general reception of the draft Regulations from public communications providers was positive […] Many responses were from members of the public opposed to the Directive on principle (24 out of 54 responses). These responses did not distinguish between the Directive and the draft Regulations on which we were consulting. Liberty, too, repeated its concerns about the Directive but did not offer substantial comment on the draft Regulations." (Home Office 2009, p. 2)*

Generally speaking, in the UK, issues like data protection and surveillance are not highly discussed topics. "Communications data retention and interception have become a non-negotiable fact of modern life. Future debate will therefore need to focus on achieving a balance between national security and intrusion into citizen's private lives."(Walker 2009, S. 333) Nonetheless, the introduction of internet data retention stemming from a European directive led to brief uproars of 'big brother' scenarios in the UK media landscape and also in scientific and NGO circles (Anderson et al. 2009, pp. 25-26). In contrast, in the UK there were even Labour government considerations published pondering an extension of data retention for content from social networks (see: Interception Modernisation Programme (Espiner 2009)). These attempts have been viewed critically, and might also lead to a higher networking and information exchange amongst European police forces (Levi/Wall 2004, p. 199). Whether the scandals of wire tapping by several tabloids, especially News of the World, will change the populace's attitudes towards the media and providers remains unclear at this point.[10]

The German government officially started the discussion about data retention after the directive 2006/24/EC[11] was issued by the Council and the Parliament of the European Union in 2006. In this directive, the fight against terrorism did not play an overriding role anymore (European Parliament/Council of the European Union 13.04.2006, p. L 105/56). It seems to be more the fight against cyber-crime that is aimed to be supported by data retention. However, the terrorism context was taken up again as a reflex action after the recent killings in Norway and an extreme right-wing terrorism scandal in Germany. On an EU-scale, the implementation into national law is up until today very fragmented. This is not only in questions of retention periods, but also in regard to legal provisions (definition of crimes, list of stakeholders) around giving out the data. The implementations were even stopped by the Czech, Romanian and German constitutional courts and have not yet been implemented by Sweden and Austria (Schweda 2011, pp. 64-70).[12]

The German implementation was made possible after Merkel's Grand Coalition came into office in 2005. The oppositional role of the former government on a European level was abandoned, even though the SPD took part in each of the two aforementioned governments. In 2007, there was a hearing during the parliamentary implementation process where most of the experts (mostly lawyers, judges, industry representatives, academics and NGOs)[13] unsuccessfully advised the federal parliament to include privacy provisions in the Bill. On top of this, the provider representatives pleaded for reimbursement, which was ignored by the parliament. The latter decision was confirmed by the *Bundesverfassungsgericht*.

[10] The recent poll mentioned before, however, still shows high credibility factors towards private companies in regards of data protection – and also in regard to data exchange.

[11] It was the fastest legislation process in the history of the Parliament of the EU so far.

[12] Similarly, different reimbursement rules for providers also exist. The harmonisation of the market seems questioned through this fact.

[13] For a detailed overview see: Deutscher Bundestag 2007

In the phase before and during the first months of German data retention, there were several large demonstrations headlined "*Freiheit statt Angst*" ("Freedom instead of Fear"), organised by data protection, human rights and Internet-related groups. Ultimately, the highest court in Germany had to follow a complaint of some 35,000 Germans after the implementation of the EU-directive. As a consequence, the act was annulled in early 2010. The court itself had asked for advice from similar stakeholders as the parliament two years before. The Chaos Computer Club was asked to advise as well, replying with a very broad and far-reaching paper (Kurz/Rieger 2009). In its decision, the court took on board significant amounts of the advice from several of the requested papers.

Since the decision of the *Bundesverfassungsgericht*, there has been strong disagreement within the CDU/CSU/Liberal government over the question of data retention. The liberal Minister of Justice is facing further calls for the re-instigation of data retention from the above mentioned stakeholders in the *Länder*, and also the SPD in federal parliament reiterated its call for it. The argumentation has changed slightly, and the fight against child pornography, organised crime and cyber crime has been raised. Surprisingly, conservative German politicians came back to the terrorism argument shortly after the recent events in Norway and intelligence scandals in Germany.

The development of data retention from the British introduction in 2000/2001 to the German annulment in 2010 demonstrates the recurring attempt of unpopular decision making via the backdoor of Europe, which is not always successful. German interest groups confronting Internet surveillance were allowed an advisory role in parliamentary legislation (without much success) and judicial consultancy (with success), which did not occur to the same extent in the UK.

Remarkably, the big parliamentary parties in Germany and the UK show a similar position and attitude towards policing the Internet and internal security, despite differences in experts' opinions. Looking at the national (and subnational) elections in the UK and Germany over the last ten years, we conclude that the main parties (Conservatives, Labour, CDU/CSU and SPD) who were in support of measures towards policing the Internet generally tended to lose voter support, whereas smaller parties gained support.[14] Parties like the Greens, who openly lobby for data protection and a free Internet, were quite successful. This led to dramatic changes in the party political landscape, especially in Germany. Whether this will lead to changes towards the securitisation of the Internet is still unclear.

5. National Institutions Struggling with the Internet

When comparing Germany and the UK, several key differences in the success of implementation of internal security measures regarding the Internet become apparent, which the example of data retention makes rather obvious. These discrepancies can be attributed (aside from cultural differences) to the diverse influence and behaviour of non-state veto players and institutions such as judicial assessments.

In Germany there are strong non-governmental actors. For instance, the Chaos Computer Club is a powerful societal actor on a European scale, and there are also several other German based NGOs focussing on data protection and Internet freedom. The German parliament and the *Bundesverfassungsgericht* requested their advice, just as the communications providers were asked for consultancy. Both actor groups submitted statements on data retention for the German Bundestag and the constitutional court. This brings both groups into a position to access and inform formally institutionalized policymaking paths. Arguably, this helps the relatively new and poor NGOs to be included in institutions of policymaking, i.e. to become institutionalised. Moreover, the CCC and other

[14] Arguably, the parties' stance towards internal security might have played some role in that context. A very recent population survey in the UK and Germany (which has not yet been published) by the SIRA Subproject 7 gives some hints as to the influence of internal security upon elections. Further information under: www.sira-security.de

NGOs are able to mobilise a relevant group of demonstrators for protest offline and online. They are able to activate an alternative lobby path via demonstrations; the 'bottom-up' paths. All in all, the NGOs involved with Internet governance have a comfortable position in Germany as they can benefit from different methods of influencing the policymaking process. It is questionable whether they can afford lobbyism in all 16 German political capitals, where decisions about Internet policing might be implemented, vetoed or put forward. Finally, the *Bundesverfassungsgericht* is increasingly becoming a part of the policy process, taking up the legislative's and executive's duty of a constitutional check against new bills in the policy field of internal security.

In contrast, the UK veto players seem weaker in their position. If one looks at the Internet providers and NGOs, they submitted advice on technical questions and questions of privacy. In the end, the providers were bought off, whereas the NGOs were basically ignored. In general, there is not a strong organisation like the CCC or a data retention-specific NGO like the *AK-Vorrat* in Germany. More importantly, the consensus on the need for and benefits of data retention seems common sense, even in NGO circles. For example, *Liberty* sees a need for data retention, whereas the *AK-Vorrat* rejects this measure in general. Parallel to Germany, the UK's Lords' Appeleate Committee (nowadays the Supreme Court) played a crucial restricting role together with the House of Lords, a role that was not taken up by Germany's second chamber but by the *Bundesverfassungsgericht* instead. In spite of these aspects, British legislation seems more rigorous. This might be connected to cultural differences and aspects yet to be uncovered, such as the populaces' and the media's attitude towards security measures online – and towards the central actors influencing and implementing these policies.[15]

References:

Anderson, Ross/Brown, Ian/Dowty. Terry/Inglesant, Philip/Heath, William/Sasse, Angela (2009). Database State. A Report Commissioned by the Joseph Rowntree Reform Trust Ltd. Under: http://www.jrrt.org.uk/uploads/database-state.pdf (checked on 4.1.2012).

Beck, Susanne (2011). Vorratsdatenspeicherung und aktuelle Entwicklungen in der Inneren Sicherheit im Vereinigten Königreich – Eine Analyse im Mai 2011. In: Bug, Mathias/Schmid, Viola/ Münch, Ursula (2011): Innere Sicherheit – auf Vorrat gespeichert? Tagungsband 2. SIRA Conference Series. Under: http://athene.bibl.unibw-muenchen.de:8081/node?id=89818, pp.87-107 (checked on 4.1.2012).

Brodowski, Dominik/Freiling, Felix C. (2011). Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Schriftreihe Sicherheit Nr. 4. Hg. v. Forschungsforum Öffentliche Sicherheit. Berlin.

Bug, Mathias/Enskat, Sebastian/Fischer, Susanne/Klüfers, Philipp/Röllgen, Jasmin/Wagner, Katrin (2011). Strategien gegen die Unsicherheit. Europäische Sicherheitsmaßnahmen nach 9/11. In: Die Friedens-Warte 86 (3-4), pp. 53-83.

Bukow, Sebastian (2009). Die neue deutsche Sicherheitsarchitektur. Wandel und Entwicklung der inneren Sicherheit in Deutschland im europäischen Kontext. In: Astrid Lorenz/Werner Reutter (Ed.): Ordnung und Wandel als Herausforderungen für Staat und Gesellschaft. Leverkusen, pp. 349–370.

Bukow, Sebastian (2011). Vorratsdatenspeicherung in Deutschland – Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests? In: Bug, Mathias/Schmid, Viola/ Münch, Ursula (2011): Innere Sicherheit – auf Vorrat gespeichert? Tagungsband 2. SIRA Conference Series. Under: http://athene.bibl.unibw-muenchen.de:8081/node?id=89818, pp. 22-55 (checked on 4.1.2012).

Büsching, Stephan (2009). Rechtsstaat und Terrorismus. Untersuchung der sicherheitspolitischen Reaktionen der USA, Deutschlands und Großbritanniens auf den internationalen Terrorismus. Frankfurt am Main.

Castells, Manuel (2005). Die Internet-Galaxie. Internet, Wirtschaft und Gesellschaft, Wiesbaden.

Council of Europe (2001). Convention on Cybercrime. Budapest. Under: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (checked on 4.1.2012).

Council of the European Union (2011). Outcome of the Proceedings of the Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party. Brussels. Under: http://register.consilium.europa.eu/pdf/en/11/st07/st07181.en11.pdf (checked on 28.3.2011).

[15] A very recent population survey in the UK and Germany (which has not yet been published) by the SIRA Subproject 7 gives some hints as to the influence of internal security upon elections. Further information under: www.sira-security.de

Crossman, Gareth; Liberty (2008). Liberty's response to the Home Office consultation paper: Transposition of Directive 2006/24/EC. Under: http://www.liberty-human-rights.org.uk/pdfs/policy08/comms-data-directive.pdf (checked on 28.03.2011).

Deutscher Bundestag (2007). Rechtsausschuss – Stellungnahmen der Sachverständigen. Under: http://webarchiv.bundestag.de/cgi/show.php?fileToLoad=1251&id=1134 (checked on 28.03.2011).

Dunn Cavelty, Myriam (2011). The Dark Side of the Net: Past, Present and Future of the Cyberthreat Story. In: AIIA Policy Commentary, No. 10, April 2011, pp. 51-62.

Dunn Cavelty, Myriam (2007). Critical information infrastructure: vulnerabilities, threats and responses. In: UNIDIR Disarmament Forum, Issue 3, 2007, pp. 15-22, http://www.unidir.ch/pdf/articles/pdf-art2643.pdf (checked on 5.8.2011).

Espiner, Tom (2009). Gov't may track all UK Facebook traffic. Under: http://www.zdnet.co.uk/news/security-threats/2009/03/18/govt-may-track-all-uk-facebook-traffic-39629479/ (checked on 28.03.2011).

European Parliament/Council of the European Union (2006). Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates. 15.03.2006. In: Amtsblatt der Europäischen Union. L 105/54 - L 105/63. Under: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF (checked on 29.3.2011).

Frevel, Bernhard/Groß, Hermann (2008). „Polizei ist Ländersache!“ – Politik der Inneren Sicherheit. In: Die Politik der Bundesländer. Staatstätigkeit im Vergleich, Wiesbaden, pp. 67-88.

Future Group (2008). Freedom, Security, Privacy – European Home Affairs in an open world. Under: http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf (checked on 5.5.2011).

Glaeßner, Gert-Joachim (2005). Großbritannien: Ein eurpäischer Sonderweg in der Politik innerer Sicherheit. In: Gert-Joachim Glaeßner und Astrid Lorenz (Eg.): Europäisierung der inneren Sicherheit. Eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus. Wiesbaden, pp. 85–106.

Government of the United Kingdom (2010). The Coalition. Our programme for government. Under: http://www.cabinetoffice.gov.uk/sites/default/files/resources/coalition_programme_for_government.pdf (checked on 14.03.2011).

Government, H. M. (2010). The Coalition: Our programme for government. Under: http://www.cabinetoffice.gov.uk/sites/default/files/resources/coalition_programme_for_government.pdf (checked on 14.3.2011).

Home office (2009). Government Response to the Public Consultation on the Transposition of Driective 2006/24/EC. Unter Mitarbeit von Andrew Knight. Hg. v. Home office. Home office. London. Under: http://www.statewatch.org/news/2009/feb/uk-data-ret-consult-response.pdf (checked on 14.11.2011).

Hornung, Gerrit/Schnabel, Christoph (2009). Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. In: *computer Law & Security Review* 25, pp. 115–122. Under: http://www.jura.uni-passau.de/fileadmin/dateien/fakultaeten/jura/lehrstuehle/hornung/Hornung___Schnabel__Data_protection_in_Germany_II__CLSR_2009__115.pdf (checked on 4.1.2012).

Krempl, Stefan/Haupt, Johannes (2011). EU-Rat plant grenzüberschreitende TK-Überwachung. In: heise online 5.1.2012, Under: http://www.heise.de/newsticker/meldung/EU-Rat-plant-grenzueberschreitende-TK-Ueberwachung-1403818.html (checked on 5.1.2012).

Krempl, Stefan/Meyer, Angela (2010). EU Kommissarin. Es bleibt bei der Vorratsdatenspeicherung. Under: http://www.heise.de/newsticker/meldung/EU-Kommissarin-Es-bleibt-bei-der-Vorratsdatenspeicherung-1147553.html (checked on 27.10.2011).

Kunz, Thomas (2004). Der Sicherheitsdiskurs. Die Innere Sicherheitspolitik und ihre Kritiker, Bielefeld.

Kurz, Constanze/Rieger, Frank (2009). Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung. Under: http://213.73.89.124/vds/VDSfinal18.pdf (checked on 5.5.2011).

Kurz, Constanze/Rieger, Frank (2011). Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Bundeszentrale für politische Bildung. Bonn.

Kutscha, Martin (1998). Große Koalition der Inneren Sicherheit. In: Bürgerrechte & Polizei/CILIP. 1. 57-69. Under: http://www.cilip.de/ausgabe/59/p-gesetz.htm (checked on 4.1.2012).

Lange, Hans-Jürgen (1999). Innere Sicherheit im Politischen System der Bundesrepublik Deutschland, Opladen.

Levi, Michael/Wall, David S. (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. In: Journal of Law and Society 31/2. pp. 194-220. Under: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6478.2004.00287.x/abstract;jsessionid=9B52666CDCE350D1626A40B0A05AE3FB.d04t04 (checked on 14.6.2011)

Malmström, Cecilia (2011). The EU Internal Security Strategy – towards a more secure Europe. Communication on Internal Security. In: The European. Security and Defence Union 2011 1/2011. pp. 18-20.

Mathiason, John (2009). Internet Governance. The new frontier of global institutions. London: Routledge (Routledge global institutions, 26).

Prätorius, Rainer (2000). Leitideen der Ausdifferenzierung der Inneren Sicherheit, in Lange, Hans-Jürgen (Ed.): Staat, Demokratie und Innere Sicherheit in Deutschland, Opladen, pp. 369-383.

Schmidt, Manfred G. (1980). CDU und SPD an der Regierung. Ein Vergleich ihrer Politik in den Ländern, Frankfurt/New York.

Schweda, Sebastian (2011). Umsetzungsunterschiede der Vorratsdatenspeicherungsrichtlinie in Europa – ein Bericht aus dem Forschungsprojekt InVoDaS im Mai 2011. In: Bug, Mathias/Schmid, Viola/ Münch, Ursula (2011): Innere Sicherheit – auf Vorrat gespeichert? Tagungsband 2. SIRA Conference Series. Under: http://athene.bibl.unibw-muenchen.de:8081/node?id=89818, pp. 56-86 (checked on 4.1.2012).

Shahin, Jamal (2007). The Reassertion of the State: Governance and the Information Revolution. In: Dun, Myriam; Krsihna-Hensel, Sai Felicia; Mauer, Victor: The Resurgence of the State – Trends and Processes in Cyberspace Governance. p. 9-34

SPD/Bündnis 90/Die Grünen (1998). Aufbruch und Erneuerung – Deutschlands Weg ins 21. Jahrhundert. Koalitionsvereinbarung zwischen der Sozialdemokratischen Partei Deutschlands und Bündnis 90/Die Grünen. Bonn.

Spittmann, Matthias (2000). Sind wir alle potenzielle Cyber-Kriminelle? Innenminister der Länder wollen Telefonverbindungsdaten noch ein halbes Jahr nach Rechnungsversand speichern. In: taz, die tageszeitung. Berlin. Under: http://blogs.taz.de/ctrl/tag/vorratsdatenspeicherung/ (checked on 11.1.2011).

Sturm, Roland (2009). Das politische System Großbritanniens, Wiesbaden.

Sydow, Gernot (2005). Parlamentssupremati e und Rule of Law, Tübingen.

Walker, Claire (2009). Data retention in the UK: Pragmatic and proportionate, or a step too far? In: *Computer Law & Security Review* 25 (4), pp. 325–334.

Wendelin, Manuel; Löblich, Maria (2011). Netzpolitik offline und online. Kommunikationsstrategien der internetpolitisch engagierten Zivilgesellschaft. In: Filipovic, Alexander/Jäckel, Michael/Schicha, Christian (Hrsg.) (being printed): Medien- und Zivilgesellschaft. Weinheim/München: Juventa.

Whitley, Edgar A./Hosein, Ian (2005). Policy discourse and data retention: The technology politics of surveillance in United Kingdom. In: Telecommunications policy 29 (11), pp. 857-874.

Williams, Chris (2010). Coalition tears up net snoop plan's £2bn price tag. Under: http://www.theregister.co.uk/2010/10/26/interception_modernisation_home_office_price/ (checked on 4.10.2011).

Zürn, Michael; Mayer, Peter (2006). Teilprojekt B4 – Abschlussbericht. Regulation und Legitimation im Internet. http://www.sfb597.uni-bremen.de/download/de/forschung/B4_2007_abschlussbericht.pdf (checked on 5.8.2011)

Abbreviations:

9/11	Terrorist Attacks in New York and Washington on the 11th of Sept 2001
AK-Vorrat	Arbeitskreis Vorratsdatenspeicherung
ATCSA	UK Anti Terrorism Crime and Security Bill
BKA	Bundeskriminalamt
CCC	Chao Computer Club
CDU	Christlich Demokratische Union
CSU	Christlich Soziale Union
ECHR	European Charter for Human Rights
EU	European Union
Eurojust	Europäische Einheit für justizielle Zusammenarbeit
Europol	Europäisches Polizeiamt
FDP	Freiheitliche Demokratische Partei Deutschlands
ICT	Information and Communication Technologies
IMK	Innenministerkonferenz

RAF	Rote Armee Fraktion
RIPA	Regulation of Investigatory Powers Act
SPD	Sozialdemokratische Partei Deutschlands
TA	Terrorism Act
UK	United Kingdom
USA	United States of America

About the Authors

Bug, Mathias

Mathias Bug is a researcher at the Institute of Political Science at the Universität der Bundeswehr in Munich, Germany. He studied Social Sciences at the Universities of Göttingen (GER), Prague (CZ), Christchurch (NZ). 2007-2010 he had scientific engagements in different political and research institutes. His research comprises Comparative Federalism, Policy Analysis (Internal Security, Migration, Education).

Röllgen, Jasmin

Jasmin Röllgen is a researcher at the Institute of Political Science at the Universität der Bundeswehr in Munich, Germany. She studied Political Science, Philosophy and History at the Universities of Cologne (GER) and Granada (ESP). Her research interests include Comparative Institutional Analysis, The New Institutionalisms, Policy Analyis (Internal Security).