Surveillance in Germany: Strategies and Counterstrategies

Ralf Bendrath, Gerrit Hornung, Andreas Pfitzmann

Delft University of Technology, University of Kassel, Dresden University of Technology

bendrath@zedat.fu-berlin.de, gerrit.hornung@uni-kassel.de, Andreas.Pfitzmann@tu-dresden.de

It is generally recognised that state surveillance of private conduct poses technical, legal and political questions at the same time. In 2008, all three dimensions culminated in Germany, when three new technical surveillance measures became subject of respective rulings of the German Federal Constitutional Court, which seized the opportunity to significantly develop the German fundamental rights system in regard to new technological developments. While the Court built upon independent expert opinion, it appears that German politicians do not understand information and communication technology well and rely too much on the opinion of actors such as the Federal Police, while ignoring that those actors have considerable self-interests, as well. On the political plane, the data retention directive and its transposition into national law has provoked the largest privacy movement ever in Germany. Besides the considerable public awareness induced by this campaign, the movement provides an interesting insight into the possibilities and restrictions of web 2.0 instruments as regards the formation of internet communities and their political activities.

Introduction

In 2008, Germany appeared to be one – if not the – point of culmination as regards the legal, technical und political discussions of new technical surveillance measures. 25 years after its groundbreaking population census decision (Bundesverfassungsgericht 1983, see Hornung and Schnabel 2009a; Rouvroy and Poullet 2009), the German Federal Constitutional Court (Bundesverfassungsgericht) delivered three important judgments on governmental surveillance and privacy in less than two weeks in early 2008, namely the "online-searching" decision (Bundesverfassungsgericht 2008a, see below), the decision on license plate scanning (Bundesverfassungsgericht 2008b), and the interim injunction to partly stop the

enactment of the European data retention directive in Germany (Bundesverfassungsgericht 2008c). In all three cases, the Court ruled against the respective measure (Hornung and Schnabel 2009b), and even established a new "fundamental right to the guarantee of the confidentiality and integrity of information technology systems" (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) in the online-searching decision.

In parallel motion, Germany has seen the formation of a new civil rights movement campaigning for personal and societal privacy. Under the motto "Freedom not Fear - Stop the surveillance mania!", the largest protest march against surveillance in German history took place in Berlin on 11 October 2008. As there were parallel activities in 15 further countries, privacy promoters in Germany hope for similar developments in Europe and beyond.

At the same time, there are strong promoters of new surveillance measures and new competences for security agencies. The most prominent among them, Federal Minister of the Interior Wolfgang Schäuble, protested after the 11 October demonstration against his portrait being used on hundreds of signs subtitled "Stasi 2.0", referring to the infamous state security service of the former GDR. As the German Federal Constitutional Court, while demanding high requirements, did not completely rule out new surveillance measures, it remains to be seen which side will prevail in the medium-term.

The aforementioned development can be addressed from very different, albeit deeply connected angels. The legal, technical and social implications have to be analysed in their respective scientific context. The first sub-chapter (by *Gerrit Hornung*) analyses the online-searching decision of 27 February 2008, concerning an Act of the Land of Nordrhein-Westfalen authorising the internal intelligence authorities to secretly access information technology systems involving the deployment of technical means. In the reasons given for the judgment, the Court established a new "fundamental right to the guarantee of the confidentiality and integrity of information technology systems", which was violated by the aforementioned provision. The second sub-chapter (by *Andreas Pfitzmann*), finds that German politicians usually do not understand information and communication technology (ICT) and therefore, often they do not understand possible uses of ICT they try to regulate. In contrast, the German Federal Constitutional Court did a remarkable job in winter and spring 2008 to decide on regulations of ICT. The last sub-chapter (by *Ralf Bendrath*), looks at the growing awareness of privacy risks and the protests which have sparked against data retention in Germany. Organizations and participants used the Internet and web 2.0 tools, which had an impact on the forms of organization, collaboration and action.

The Online Searching Judgement of February 27th, 2008

Gerrit Hornung

The strength of the German constitutional system as regard new technological developments became very visible in the spring of 2008, when the German Federal Constitutional Court delivered three important judgments on privacy (or informational self-determination, as developed by the German federal Constitutional Court in the population census decision) and new surveillance technologies (on the following, see Hornung and Schnabel 2009b). Arguably, the most important of these decisions is the judgment on the online searching of computers, which established a new "fundamental right to the guarantee of the confidentiality and integrity of information technology systems". The birth of this fundamental right led to an ongoing scientific debate in Germany (see, e.g., Böckenförde 2008, Hoffmann-Riem 2008; Hornung 2008; Roggan (ed.) 2008; Roßnagel and Schnabel 2008), but the decision was also recognised in other countries (see, e.g., Abel and Schafer 2009; de Hert, de Vries and Guthwirth 2009).

Background of the Case

The online searching case concerned an Act by the state of Nordrhein-Westfalen which authorised the Office for the Protection of the Constitution of the State (internal intelligence authorities) to, *inter alia*, "secretly access information technology systems through the use of technical means" (on the background, see also Abel and Schafer 2009, pp. 107 ff.; Abel 2009, pp. 99 ff.). The fact that no further indications were given regarding the mode of access gave rise to speculations on the potential technical approach. Possibilities include one-time online access to the data on the computer, continuous surveillance to tape-record any change of such data, and the observation of further operations (such as keyboard entries or VoIP calls, see Buermeyer 2007).

Most observers had expected the German Federal Constitutional Court to rule against the state of Nordrhein-Westfalen, as the Act suffered from a considerable lack of substantial and procedural privacy safeguards. This impression was fostered in the oral proceedings. Hardly anybody however would have expected the Court to come up with a "new" fundamental right. This right is strictly speaking not a new constitutional right, but a new sub-group of the general personality right (see Hoffmann-Riem 2008, pp. 1018 f.). Arguably, the creation of a new right by the Court would have given rise to issues of the separation of powers. In practice however, the future approach of the Court may outweigh the difference between a specific right and a sub-group of the general personality right. As apparent from the development and impact of the right to informational self-determination (another sub-group of the general personality right), the German Federal Constitutional Court does not hesitate to use a non-written fundamental right to severely restrict surveillance activities by state agencies.

Other Fundamental Rights

As to the merits, the German Federal Constitutional Court took the recent developments in the area of information and communication technology as a starting point (Bundesverfassungsgericht 2008a, pp. 303 ff.; see Hoffmann-Riem 2008, pp. 1010 ff.; Hornung and Schnabel 2009b). Much emphasis is placed on the major role played by these kinds of technology in today's life and their ever increasing influence on the self-development of citizens. As the new technology depends largely on the processing of personal data, it has become obvious that there is a strong need for the protection of privacy. The Court did not consider the existing German system of fundamental rights (as explained above) to be sufficient in this respect. Secrecy of telecommunications, as protected in Article 10 of the Grundgesetz, did not cover online searching of computer systems (see also Abel and Schafer 2009, pp. 112 ff.). The Court considered secrecy of telecommunications as being applicable only if the authorities aim at the surveillance of VoIP systems, and the method of the surveillance (e.g., a Trojan horse or similar malware) is technically restricted to the telecommunications, i.e., searching of the system is not possible.

Regarding the sanctity of the home, there was a debate on whether the respective provision of the Grundgesetz (Article 13) applies in the case of the online searching of an IT system which is based in the home of the person affected. While there are solid arguments that this is the case (Hornung 2007, pp. 577 f. with further references), the German Federal Constitutional Court (Bundesverfassungsgericht 2008a, pp. 309 ff.) responded negatively, arguing that the location of the system is not usually apparent for the authorities, and that the fundamental right in Article 13 of the Grundgesetz has to be construed with regard to the modalities of the access. Lastly, the German Federal Constitutional Court (Bundesverfassungsgericht 2008a, pp. 311 ff.) deemed the right to informational self-determination as not covering the peculiarities of IT systems and their relevance for citizens' everyday lives. This last part of the decision has been widely criticized among scientific scholars and may indeed be the weakest part of the judgment. Before the decision, hardly anybody would have doubted that secret online searchings of computers interfere with the right to informational self-determination. Thus, the Court arguably construed a lacuna in the constitutional system of fundamental rights to fill it with the right to the guarantee of the confidentiality and integrity of information technology systems. On the other hand, the political and semantical value of a specific fundamental right for the "information age" should not be underestimated (Abel and Schafer 2009, pp. 122 f.).

Content of the "new" Fundamental Right

Having dealt with the other fundamental rights, the Court emphasised what it calls the "loophole-closing guarantee of the general personality right" (Bundesverfassungsgericht 2008a, p. 313). From there, it was only a small step to the creation of a new sub-group, protecting "IT systems which alone or in their technical net-

working can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of the personality" (Bundesverfassungsgericht 2008a, p. 314). Besides computers, mobile phones, PDAs and similar systems are also included if they "have a large number of functions and can collect and store many kinds of personal data" (see also Abel and Schafer 2009, pp. 120 f.). Crucially, it is not decisive whether the system actually stores or processes personal data to that extent, but whether the system is capable in that respect.

The system will only be protected if, given the concrete circumstances, the person affected can assume that he/she is able to control the system, whether alone or with other authorised persons. Arguably, this also includes online hard drives (Hoffmann-Riem 2008, p. 1012).

There are two aspects of the new right, namely, the confidentiality and the integrity of the system. The first aspect covers personal data and is thus largely congruent with the right to informational self-determination, although the requirements for interventions are much higher. The second aspect is described by the German Federal Constitutional Court to protect against the unauthorised use of the system regarding its capacities, functions and memory contents. In this respect, it is irrelevant whether personal data of any kind is involved.

Interferences

The Court did not consider the fundamental right to be absolute, but specified rather high requirements for any interference by public authorities (on the situation in the UK, see Abel 2009, p. 104). Importantly, these requirements apply to both the police and intelligence agencies. In both cases, there have to be "factual indications of a concrete danger to a predominantly important legal interest. Predominantly important are the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence." (Bundesverfassungsgericht 2008a, p. 328). The requirement of "factual indications of a concrete danger" had been unknown in traditional German police law. It is arguably placed between the concrete threat itself and the general gathering for information, but there are indications that the Court will require public authorities to firmly establish factual evidence connected to individual persons.

Even if there is such evidence, the interference can only be justified if it is warranted by a judge or a body of equal legal and personal independence (see Hornung and Schnabel 2009). Furthermore, the legal basis for the measure has to provide safeguards to prevent any infringements of the "core of personal privacy" as developed in the decision on acoustic surveillance of private homes (Bundesverfassungsgericht 2004, pp. 311 ff.). In the current case, the German Federal Constitutional Court considered it impossible to analyse the data, in this respect, at the time of collection. According to the technical experts in the Court session, there

are no technical means which would absolutely exclude data belonging to the core of personal privacy from the transfer to the authorities. In this situation, the judges demanded that the data is subsequently examined in this respect and deleted if it pertains to this sphere. However, there are neither indications in the judgment as to the body responsible for the examination, nor to the time within which the examination must take place. The new federal law which allows for the secret searching of IT systems (section 20k of the Bundeskriminalamtgesetz of 25 December 2008) requires the control of an independent judge. However, the examination itself will be conducted by the federal police, including its data protection officer. This new law has already been challenged before the German Federal Constitutional Court, and it remains to be seen whether the Court considers these safeguards to be sufficient.

Further Developments

The opinion of the German Federal Constitutional Court delivers guidelines not only for the online searching of computer systems, but also for other surveillance measures. Hence, the ruling is widely recognised as the most important decision on privacy and constitutional law in Germany within recent years, arguably even since the famous census case of 1983. There are numerous open questions to be addressed in future cases and in the scientific debate (Hornung and Schnabel 2009; Hornung 2008). These include, *inter alia*, the consequences for open searches of IT systems (Hömig 2009, p. 210 f.), further dimensions of the new fundamental right in regards to the effects between private parties (Roßnagel and Schnabel 2008), and the issue of online searching of IT systems within criminal proceedings, which was not addressed by the Court in the current decision.

On the international plane, it remains open whether other constitutional courts will follow the approach of the German Federal Constitutional Court. Among other factors, this will depend on the role of the court in the respective constitutional system and the existence of a general personality right or right to privacy which can be developed to address the new challenges in a world of widespread use of IT systems. As the European systems of fundamental rights protection become more and more important, it will be of even more relevance whether the European Court of Human Rights and the European Court of Justice take up the ideas and concerns expressed by the German judges.

The German Federal Constitutional Court - Closer to ICT and Technology Assessment than German Politicians

Andreas Pfitzmann

German government executives usually do not understand information and communication technology (ICT) well and therefore, often they do not understand possible uses of ICT they try to regulate (and some politicians are even proud of not understanding ICT). So, the German government, e.g., assumes terrorists will connect their computers to the Internet in an insecure fashion so that the German Federal Police can search their hard drives secretly (section 20k of the Bundeskriminalamtgesetz of 25 December 2008).

In spite of this attitude of the German government, the German Federal Constitutional Court did a remarkable job in Winter and Spring 2008 to decide on regulations of ICT. This section shortly explains why and how.

I admit from the outset that all conclusions are my personal ones based on my own experience in directly interacting with politicians in various roles, e.g., being asked to give consultancy and advice to many politicians, to three political parties being elected into German Parliament (Bundestag) and to several political bodies for more than two decades. I have been expert witness in parliamentary hearings as well as in trials of the German Federal Constitutional Court dealing with issues described in this section.

Actors and their Knowledge

For German politicians (at least those of the larger parties), understanding ICT is not “sexy”. For them, understanding ICT is as attractive as understanding mathematics and having been a nerd at school. German politicians fear that the electorate would perceive them as too detached if politicians knew much about mathematics and ICT. This would thwart their success in elections, they believe. Nevertheless, German politicians admit that society is on its way to become an information society.

So far, it would not be much of a problem, if German politicians drew the consequences of their very limited understanding of the digital space and mainly refrained from trying to regulate it.

In spite of not understanding ICT, German politicians firmly assume that ICT does what it shall do. The more knowledgeable amongst them believe that if ICT systems have some errors or security weaknesses in their first release, these bugs will be fixed soon. Overall German politicians firmly assume that whatever policies they make, these policies can and will be enforced effectively.

So, German politicians act according to this rule: if you lack understanding and experience to rely on, do something and pretend you are certain to do the right things.

Since ICT is not really new (at least for the younger generation), it may well be that the German government has on average better knowledge than society at large, but the German government quite likely has on average less knowledge about ICT than society at large, in particular the younger generation, cf. Fig. 1.

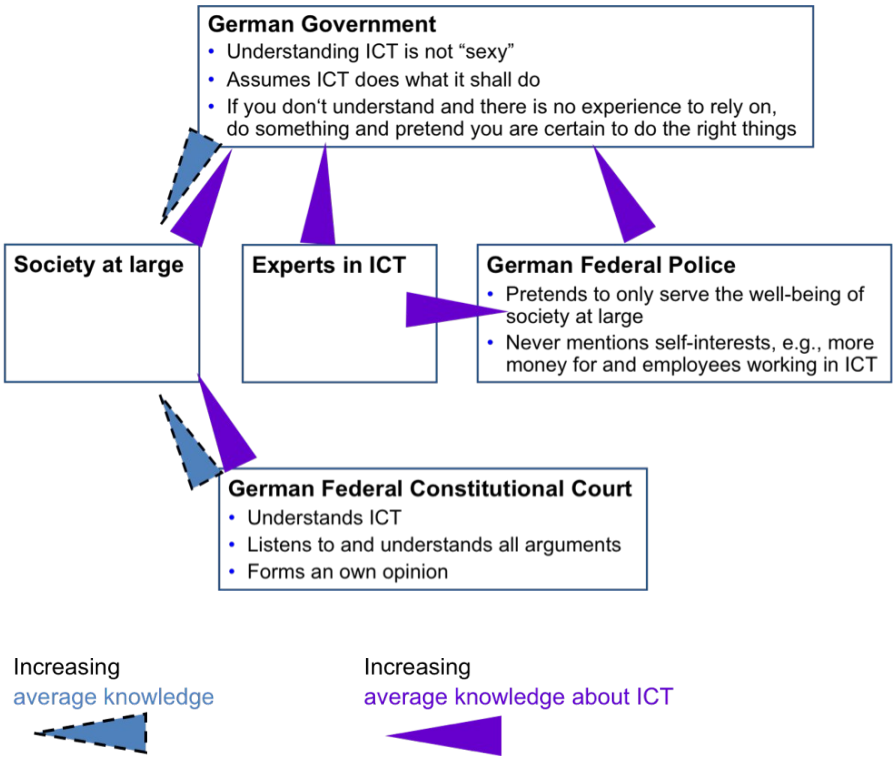

Fig. 1: Actors and their knowledge

Let's complete the picture with two more assertions:

Obviously, experts in ICT are on average much more knowledgeable of ICT than even the ICT-interested members of the government.

The German Federal Police has a better understanding of ICT than the German government, but less understanding about ICT than independent experts in ICT, e.g., from academia.

The problem now is that the German government has so little knowledge about ICT that its members do not dare to build up an own opinion about the use of ICT with respect to surveillance vs. privacy, fighting crime vs. supporting development of society. So they decided to completely rely on the advice given to them by the most knowledgeable governmental bodies. For fighting crime, e.g., this means fully relying on the advice by the German Federal Police. This makes life for politicians as easy as possible, since it avoids being criticized by the police. And it enables German politicians to pretend to do everything which is possible for fighting crime and terrorism as well as providing as much public safety as possible. But of course, the German Federal Police, though pretending to only serve the well-being of society at large, has some self-interests, which are barely mentioned. They include more money and more employees working at the German (Federal) Police in

the area of ICT. These usually come along with additional rights and duties. This is a serious downside of our government's approach: more data stored for use by our police and our secret services does neither mean more security nor more public safety. This is so because foreign secret services as well as organized crime will gain access to these retained data quite likely and relatively soon. The same is true for all security holes not closed as fast as possible due to the interests of, e.g., the German (Federal) Police to further use them for online-searching of suspects' computers. Another downside is that this way, privacy of citizens is largely ignored.

To sum up so far: Due to the lack of knowledge of ICT in the German government, society at large is paying with their privacy (and a lot of money, not to completely ignore it) for an uncertain increase in security and public safety. Not a good deal, quite sure. Unavoidable? Probably not, since, first, society at large, meanwhile more knowledgeable about ICT than the German government, will sooner or later elect only politicians into office who are computer-literate, and, second, the German Federal Constitutional Court comes into play.

Over more than two decades, I gave consultancy and advice to many politicians, political parties and political bodies. But I never ever experienced so much interest in understanding ICT as when being expert witness to the German Federal Constitutional Court. Its judges really wanted to understand ICT astonishingly deeply. They really did read the papers I wrote for them – and even more: they read and understood even the papers I recommended to them. For me as a computer expert, it was a unique experience to listen to the court's introductory statements, devoting more than 5 minutes to the fundamental issues of ICT, and having the strong feeling that I myself could not have presented it more clearly. This in complete contrast to listening to leading German politicians, who if not in their first sentence addressing ICT, then in their second sentence reveal their serious misunderstandings of fundamental properties of ICT.

In the court hearing, the judges listened to all arguments and made sure they understood them. The judges further made sure the experts did discuss their arguments with each other in their presence (and sometimes moderated by the judges or forced by the judges to stick to the point). This is something the German parliamentary system avoids wherever possible. Overall, by the way the judges prepared and organized the court hearing, they ensured to be able to form a valid opinion of their own, taking both the fundamental properties of ICT into account as well as the self-interests of all parties involved.

Given this distribution of knowledge, what are the strategies of those working unconsciously or consciously against privacy? And what could be appropriate counterstrategies? Overall: How might we arrive at a realistic technology assessment of ICT being a basis for good decisions with regard to the future ICT infrastructure for our society?

Strategies Working against Privacy and Appropriate Counter-strategies Working towards Privacy

The main strategy working against privacy is in actors who receive resources for law enforcement, who have self-interests (which are never mentioned), but who are able to pretend that they only serve the well-being of the society at large, as well as being the sole advisors to the government. The main cause for this is that the government is not able to really listen to more than one "expert", since it has no own judgement and so no capability to sort out contradictions between "experts".

The counterstrategies are:

- Make sure politicians including government officials have to take some training in ICT. Not understanding the technological basis of the future society should no longer be acceptable for leaders of any kind. Experts should prepare several courses at the appropriate levels of detail including basic knowledge to understand the shortcomings of ICT with regard to security. As mentioned, this understanding is an essential precondition to understand that in the foreseeable future, ICT will not just do what it shall do – this is a message mainly academia has to spread, since neither German Federal Police nor industry surely have any interests to spread that message.

- German Federal Police should be offered in-depth training in ICT in general and ICT-security in particular. Since it may well be that currently they do not know how bad their proposals actually are with regard to increasing security and public safety.

- In addition, procedures in public hearings, e.g., in the German parliament (Bundestag) should be revised such that not only politicians can ask questions to experts, but that the experts themselves can challenge other experts' statements. This is particularly necessary if some of the "experts" are not independent, but officials of governmental bodies, e.g. of the German Federal Police, having self-interests.

Summing up: Government vs. Court

The knowledge of ICT of the German government is much weaker than the knowledge the German Federal Constitutional Court acquired within a relatively short period of time. So in principle, there is hope that people are able to learn.

Is, what I described, specific to ICT? Probably yes:

- Experience in physical life is not always applicable in the digital space. Therefore, older leading politicians have no basis to decide appropriately in matters regarding the information society.

- Having no knowledge in ICT was socially accepted (and convenient). Hopefully, this is to change quite soon.

Is, what I described, part of a strategy? Maybe it is a strategy of some bureaucrats within government in general and police and secret services in particular. I do not believe it is an explicit strategy of many politicians. With regard to them, it is just an outcome of ignorance.

Is, what I described, an institutional necessity: fight for resources at the cost of freedom? Maybe. And at the moment, we have much more powerful actors who, in their fight for resources, decrease privacy than we have actors who advocate spending resources on privacy protection.

To conclude, appropriate counterstrategies are:

- Government needs training in ICT.

- Make sure that self-interests are disclosed in an open debate.

The Rise of the Anti-Surveillance Movement 2.0

Ralf Bendrath

This sub-chapter analyzes the new forms of privacy activism that have emerged in Germany around the fight against telecommunications data retention. It provides an explorative case study of the new "activism 2.0" that heavily relies on user-participation, flat hierarchies, and distributed collaborative work as described by authors like Benkler (2006) and Shirky (2008). The case also illustrates some of the challenges connected to these new forms of organizing and political campaigning.

Almost 30 years ago, West Germany already saw the emergence of an active anti-surveillance movement. It mainly fought against the planned nation-wide census, which was seen by many as the entry into the big brother state. Broader issues debated in this context in the 1980s were police surveillance repression against social movements, such as the anti-nuclear movement, the peace movement, the new left, and the squatter community. The 1983 Federal Constitutional Court decision against the census established a new basic right to "informational self-determination" (Bundesverfassungsgericht 1983), but also took the drive out of many of the anti-censorship activists. Together with the integration of the social movements into the parliamentary system of the Federal Republic through the Green party, this took surveillance and data privacy off the streets as well as off the agenda of many groups.

A few years later, the East German opposition that finally led to the fall of the Berlin wall in 1989 was not only a democratic movement, but also was much mobilized by a common rejection of surveillance as a means of the dictatorship. A

crucial event was the storming of the Stasi headquarters in East Berlin on 15 January 1990, which finally led to the securing of the Stasi archives and the later establishment of the related Federal Agency ("Gauck Commission"). After the German re-unification, the concerns of the former opposition groups were largely seen as not necessary anymore.

From late 1990, there was basically no widespread privacy movement anymore in Germany. Only a few NGOs, such as the German Association for Data Protection (DVD), the Computer Scientists for Peace and Social Responsibility (FIfF), the "Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V." (FoeBuD), the Humanistic Union (HU) and the hacker association Chaos Computer Club (CCC), kept on working on these topics. They tried to fight some of the new surveillance measures, which were introduced as a means in the fight against "organized crime", such as the bugging of private houses, which became know as the "big eavesdropping attack". Too weak for political successes, the privacy groups mainly resorted to constitutional challenges of new surveillance laws. Only ten years later, the German Big Brother Award was born in 2000 and is now in its 10th year.

Data Retention and the participatory Resistance against Surveillance

After the events of 9/11 2001, many liberal and left-wing groups as well as the traditional privacy community were feeling a general unease with the new repressive tendencies and surveillance measures. Politically, the anti-terror climate made it hard for them to find much support among the population as well as attention in the media (Bendrath 2001). As a consequence, protest and criticism against many of the supposed anti-terror measures were mainly published and debated in specialized internet forums, but without much political output and even less impact. With the help of this new medium however, the small privacy community was able to exchange news and analyses, stay in touch throughout the dire years, and find new followers among the "internet generation". It took a number of years before a larger opposition against surveillance rose again and finally even placed its concerns high up on the national political agenda.

The turning point was the introduction of the EU data retention directive (EU 2006). Groups like European Digital Rights (EDRi) and Privacy International had tried to fight against the blanket storing of all telecommunications traffic data in the European Union since 2003, but without much success. When it was finally adopted by the European Parliament on 14 December 2005, German privacy activists immediately knew that it would now hit the national level for transposition into German law. The interesting and extraordinary story of how they successfully organized their protest and activities with the help of new online tools tells us something about the value of the internet for social movements in the information age.

The initiative that later became known as the Working Group on Data Retention ("Arbeitskreis Vorratsdatenspeicherung" or short "AK Vorrat", www.vorratsdatenspeicherung.de) started on the internet itself. Hundreds of readers of the popular IT news service heise.de commented on the article that reported about the European Parliament's decision, expressing their anger and outrage. Many of them understood that this legislative measure for the first time put everybody under surveillance, no matter if there was an initial suspicion or not. They feared that telecommunications traffic was only the beginning and that without large opposition, sooner or later more and more behavioral data of the whole population would be retained and made available to security agencies. Privacy activist Bettina Winsemann (also known as "Twister", who also was one of the complainants in the online searching decision) from the small group "Stop1984" offered those of them a home on their listserv who wanted to do more than just rail against the decision in some online forum. On the listserv, their feeling of unease and the will "to do something" was facilitated and slowly turned into more organized forms with the help of some more experienced privacy activists. These also organized a first face-to-face meeting of the group at the CCC congress in Berlin two weeks later.

AK Vorrat initially had no campaign plan, no money, no staff, no organizational form, and no real infrastructure except for the listserv. It did not even have its name at the beginning. But this lack of resources and fixed structures, interestingly, turned out to be an asset. It forced the activists to set up the infrastructure themselves and to develop the campaign collaboratively and iteratively. Someone had a wiki that was used for the first months, others were experienced in graphics design, someone knew a legal expert who had worked on data retention, others were familiar or at least interested in press relations, and so on. With the extremely open set-up of an un-moderated listserv and a wiki, anybody wanting to help could help, in the area of his or her expertise or interest. This created "ownership" and the sense of a community of peers. Through some more popular German blogs, such as netzpolitik.org, word of AK Vorrat spread in the internet community and slowly made it bigger, stronger, and more organized.

The first ideas AK Vorrat's members came up with were focused on mobilizing the wider German internet community through participatory means. They created banners, graphics and widgets (small javascript applets) that others could incorporate in their websites and blogs. They also set up a web portal where anybody could write an open letter which would automatically be sent to the members of the ruling conservative and social democratic parties in the federal parliament. Exactly one year after the European Parliament had adopted the data retention directive, AK Vorrat provided a symbolic death notice in traditional design with big black letters and an ark frame, which commemorated the "death of privacy" twelve months before. It was taken up by many bloggers and website owners who put it before their start page. For many months, the press releases were largely ignored by the mainstream media, but were distributed and linked to in a growing number of blogs. This, in turn, motivated more internet users to join the group.

The growth of AK Vorrat led to a gradual internal differentiation over time. The activists organized themselves in specialized working groups for design, server maintenance, press work, translations, wiki housekeeping and other areas. After one year and with more than 1,000 members on the listserv, the activists also started to set up local chapters. Still, most of the work was coordinated in the wiki (wiki.vorratsdatenspeicherung.de), which made is easy for anybody to set up a local group or coordinate an activity without the need for central discussion or even approval.

From the Internet to the Streets and into Pop Culture

The privacy activists understood early on that if they wanted to be successful, they would have to reach out of the internet community and towards other social groups. They initiated a joint declaration – a manifesto on the dangers of data retention – that was send to other NGOs for signature. Initially, mainly privacy and legal experts groups as well as some consumer and journalists' organizations signed the declaration, but after a while, groups such as the German AIDS Help, the German Association for Sociology, or the Federal Association of Women Help-Lines also joined. They had understood that their work would also be affected by the blanket retention of telecommunications data.

For the activists, this was not enough. When it was reported that the German Parliament would discuss data retention in late June 2006, they immediately started to organize a street demonstration on the Saturday before. With only about three weeks of preparation and mobilization time, only 250 protesters showed up and marched through downtown Berlin. While this demonstration had – foreseeable – no media coverage at all, it showed the activists two things: First, they were not alone, and demonstrations could be a good way of meeting more like-minded people in person. Second, it was easy to do a demonstration if the workload could be distributed through wikis and listservs. As a consequence, AK Vorrat called for and organized more demonstrations over the next year. The second one took place in Bielefeld on the afternoon before the Big Brother Awards ceremony 2006 took place with 350 participants. It was also the first one that had as its motto "Freedom not Fear" ("Freiheit statt Angst"), which expressed the motivation of the privacy activists very well and later became the slogan for internationally coordinated activities. The third demonstration was organized in Frankfurt in April 2007. Here, already 2,000 people showed up on the streets, indicating the growing mobilization for privacy and against surveillance. In order to root privacy better in the population, AK Vorrat also started the platform freiheitsredner.de ("freedom speakers"), where activists could register and indicate their willingness to give talks about surveillance and privacy for school classes, political initiatives and whoever else was interested.

The last push towards a mass movement came in 2007. The Federal Minister of the Interior, Wolfgang Schäuble, had announced a lengthy catalogue of planned new surveillance measures, including the secret online searches of private hard

drives through malware, widely known in Germany as the "federal Trojan" (see above). Shortly after this, activists of AK Vorrat were taking part in the first big German-wide blogger and web 2.0 conference, re:publica in Berlin. They ran a workshop on activism against surveillance and called for the web-design and web 2.0 communities to come up with creative ideas and campaign elements. An idea was to tag all blog posts related to Schäuble with "Stasi 2.0", a meme that had originally been invented as early as July 2001 in an online forum (NBX 2001). Dirk Adler, co-author of the blog dataloo.de, took part in the workshop at re:publica and came up with a stylized picture of Wolfgang Schäuble and the slogan "Stasi 2.0" in capital letters below it (Adler 2007). This logo became widely known as the "Schäublone" and was extremely popular in the German blogosphere. Adler also sold it on clothing and mugs through a web 2.0 shop at dataloo.spreadshirt.net. He donated part of his revenue to AK Vorrat, and spreadshirt did the same for a couple of months in 2007.

The combination of pop culture coolness, the substantial work of Ak Vorrat and others, and a more and more politicized blogosphere, created a fertile ground for the first large-scale manifestation of the new privacy movement. With the donations from the t-shirt sales, AK Vorrat and a coalition of more than 50 groups and organizations called for another demonstration in Berlin on 22 September 2007. In the end, under a blue sky and a nice autumn sun, 15,000 protestors marched through Berlin and held their final rally right in front of the Brandenburg Gate. From this day it was clear that Germany again had a mass movement against surveillance and for privacy.

Putting Privacy on the political Agenda

The following year of 2008 can be marked as the year where privacy moved high on the public agenda in Germany. On 1 January, the law on data retention went into effect, which made Germany drop from number one to seven in the country ranking published by Privacy International. At the same day, a constitutional challenge was submitted to the German Federal Constitutional Court. AK Vorrat and its allies again had focused on participatory methods, based on the fact that in Germany, a constitutional challenge does not involve any court fees. Through an online form, they had managed to have more than 34,000 people participate in this case – the largest constitutional complaint ever seen in German history. The paperwork had to be brought to the Federal Constitutional Court in huge moving boxes, which also offered a nice photo opportunity for everyone wanting to demonstrate how many people oppose data retention.

In February, the media reported widely about the Federal Constitutional Court's decision on secret online searches (see above). In March, the Chaos Computer Club published the fingerprint of the Federal Minister of the Interior, Wolfgang Schäuble. This sparked high public attention, made front page news even in the tabloid press, and proved that biometric authentication as introduced in the German passport and identity card is not safe at all. Inspired by the successes, the

growing number of privacy activists held a de-central action day in May 2008. Different kinds of activities, like demonstrations, flash mobs, information booths, privacy parties, workshops, and cultural activities took place in all over Germany.

Over the summer, some of the biggest German companies "helped" in raising public awareness of the risks of large data collections. Almost every week, there were reports on a big supermarket chain spying on its employees, on cd-roms with tens of thousands of customer data sets from call centers – including bank account numbers – being sold on the grey market, on the largest German telecommunications provider using retained traffic data for spying on its supervisory board and on high-ranking union members, on an airline using its booking system to spy on critical journalists, on two large universities accidentally making all student data available online, or on a big mobile phone provider "losing" 17 million customer data sets.

The Federal Government, under building public pressure, introduced some small changes for the federal data protection law, but at the same time continued its push for more surveillance measures in the hands of the federal criminal agency (Bundeskriminalamt, BKA). These included the secret online searches the constitutional court had just cut down to very exceptional circumstances a few months earlier. The German public discussed these moves very critically, especially since journalists are exempted from special protections that are given to priests, criminal defense lawyers, and doctors.

Because of the public concern and debate about privacy risks, the call to another mass street protest was even more successful than ever before. The "Freedom not Fear" action day on 11 October was the biggest privacy event in Germany's history. In Berlin, between 50,000 and 70,000 persons protested against data retention and other forms of "surveillance mania". Privacy activists in many cities all over the world participated with very diverse and creative kinds of activities and turned this day into the first international action day "Freedom not Fear". The anti-surveillance protests finally kicked off some serious discussion within the Social Democratic Party (SPD) in a number of the German states. This resulted in a loss of the majority for the law on the federal criminal agency (BKA) in the second chamber (Bundesrat) in the first vote. It only was passed weeks later, after some changes were introduced, and with heavy pressure from leading federal Social Democrats. The new law is still seen as unconstitutional by many legal and privacy experts, and in January 2009 a case was submitted to the Federal Constitutional Court. Related activities are still going on all over Germany, and AK Vorrat is by now only one of the players in this movement – others have been inspired by it, but have started their own activities and actions.

Lessons learned

The basis of the success of the new privacy movement was its openness. The reliance on open structures and as little hierarchy and central points of control as possible made it easy for anyone to participate and created ownership. An addi-

tional factor was the maturing of the political German blogosphere, with specialized blogs such as netzpolitik.org being highly successful, but also other, previously non-political blogs slowly becoming politicized. It also has proven very helpful to go offline. Online tools were used to set up local structures and to get the protest offline, to the streets and into pop culture. The use of creative commons licenses was crucial here, because the "Stasi 2.0" logos as well as other material could therefore be used by anyone. Overall, the (involuntary) founding idea was proven right: Give people an environment in which they can do what they are good at, and give them tools to coordinate and help each other.

Not all of the success was due to web 2.0, though. Even in times of distributed and nowadays even twitter-based activism, where whole campaigns are glued together by one hashtag, experts are still relevant. If AK Vorrat had not been lucky to get on board legal experts such as Patrick Breyer, who had written his legal dissertation on data retention and was crucial for much of the substantive work, the campaign had never gotten as far as it went – especially not to the constitutional court. The activism also needed the help of established NGOs for logistics: FoeBuD provided their online shop for the distribution of flyers, posters and other material; tax-exempt FIfF was donating a bank account and the management of donations and financial contributions.

Of course, such a working environment also creates problems. One lesson quickly learned by the activists was that fluid and open structures create a constant need for discussion about the whole nature of AK Vorrat. Is it a new form of organization? Is it a coalition of established NGOs, many of whom worked inside this new structure? Is it a platform for free-floating activists? Is it a network of like-minded activists? Or is it even all of the above? The activists also had to learn the hard way that decisions and debates about highly political issues (such as the participation of militant left-wing groups in the demonstrations) are hard to hold online and involve a constant danger of escalation and flame-wars. The un-moderated listserv also made it hard to participate for people who are used to more focused and traditional means of communications or who represent more established and formalized organizations such as trade unions. Much of the work of the more experienced privacy activists (including the author Ralf Bendrath) therefore has been in facilitating discussions and leading not by orders, but by listening and moderating. Still, the discussions and internal conflicts have led some activists to turn away from AK Vorrat and set up their own organizations and groups. While this is seen by many activists as a loss of coherence or even as betrayal, in the bigger picture, it can also be interpreted as the growing pains of a maturing social movement. Privacy is on the political agenda again in Germany, and there are no signs of it fading anytime soon.

References

Abel, W. (2009), Agents, Trojans and tags: The next generation of investigators, International Review of Law, Computers & Technology 2009, pp. 99-108.

Abel, W. and Schafer, B. (2009), The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822, 6:1 *SCRIPTed* 106, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

Adler, D. (2007), Stasi 2.0, dataloo.de, 14 April, http://www.dataloo.de/stasi-20-525.html.

Bendrath, R. (2001), Wie weiter mit dem Datenschutz? Telepolis, 24 October, http://www.heise.de/tp/r4/artikel/9/9903/1.html.

Benkler, Y. (2006), The Wealth of Networks. How Social Production Transforms Markets and Freedom, New Haven and London.

Böckenförde, T. (2008), Auf dem Weg zur elektronischen Privatsphäre, Juristenzeitung 2008, pp. 925-939.

Buermeyer, U. (2007), Die Online-Durchsuchung, HRR-Strafrecht 2007, pp. 154-166, http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8.

Bundesverfassungsgericht (1983), Decision of 15 December 1983 (1BvR 209, 269, 362, 420, 440, 484/83), decisions volume 65, pp. 1-71.

Bundesverfassungsgericht (2004), Decision of 3 March 2004 (1 BvR 2378/99 and 1 BvR 1084/99), decisions volume 109, pp. 279-391 (also available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html).

Bundesverfassungsgericht (2008a), Decision of 27 Feburary 2008 (1 BvR 370/07 and 1 BvR 595/07), decisions volume 120, pp. 274-350 (also available in English at http://www.bverfg.de/en/decisions/rs20080227_1bvr037007en.html).

Bundesverfassungsgericht (2008b), Decision of 11 March 2008 (1 BvR 2074/05 and 1 BvR 1254/07), decisions volume 120, pp. 378-433 (also available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html).

Bundesverfassungsgericht (2008c), Decision of 11 March 2008 (1 BvR 256/08), Europäische Grundrechte Zeitschrift 2008, pp. 257-265 (also available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html).

De Hert, P., de Vries, K. and Gutwirth, S. (2009), La limitation des 'perquisitions en ligne' par un renouvellement des droit fondamentaux", Note d'observations sur Cour constitutionnelle fédérale allemande, 27 février 2008 (Online Dursuchung), Revue du droit des Technologies de l'Information, Jurisprudence, 2009, pp. 89-92.

EU (2006), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105 , 13/04/2006 pp. 0054 - 0063.

Hömig, D., "Neues" Grundrecht, neue Fragen? Zum Urteil des BVerfG zur Online-Durchsuchung, JURA 2009, pp. 207-213.

Hoffmann-Riem, W. (2008), Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, Juristenzeitung 2008, pp. 1009-1022.

Hornung, G. (2007), Ermächtigungsgrundlage für die 'Online-Durchsuchung'?, Datenschutz und Datensicherheit 2007, pp. 575-580, available at http://www.uni-kassel.de/fb7/ oeff_recht/publikationen/pubOrdner/publikation_2007_hornung_online_durchsuchung.pdf.

Hornung, G. (2008), Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integrität informationstechnischer Systeme", Computer und Recht 5/2008, pp. 299-306.

Hornung, G. and Schnabel, C. (2009a), Data protection in Germany I: The population census decision and the right to informational self-determination, Computer Law & Security Review 2009, pp. 84-88.

Hornung, G. and Schnabel, C. (2009b), Data protection in Germany II: Recent Decisions on Online-Searching of Computers, Automatic Number Plate Recognition and Data Retention, Computer Law & Security Review 2009, pp. 115-122.

NBX (2001), Stasi 2.0, 7 July, comment in telepolis, http://www.heise.de/tp/foren/S-Stasi-2-0/forum-18164/msg-815528/read/.

Roggan, F. (Ed., 2008): Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin 2008.

Roßnagel, A. and Schnabel, C. (2008), Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, Neue Juristische Wochenschrift 2008, pp. 3534-3538.

Rouvroy, A. and Poullet, Y. (2009), The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy, in: Gutwirth, S.; Poullet, Y.; De Hert, P.; de Terwangne, C.; Nouwt, S. (Eds.), Reinventing Data Protection, forthcoming.

Shirky, C. (2008), Here Comes Everybody: The Power of Organizing Without Organizations, New York.