

Privacy Activism after Snowden: Advocacy Networks or Protest?

Sebastian Haunss

Privacy, i.e. the protection of unauthorized access to personal data, is a widely discussed issue today. Fueled by Edward Snowden's revelations about the US National Security Agency's, the British Government Communications Headquarters', and other national secret services' all-encompassing and blanket surveillance practices, on the one hand, and by frequent reports about major data leaks from government and private websites, on the other hand, privacy issues remain highly visible in the news media. Contrary to the provocative interjections by some authors that we already live in a post-privacy era (Heller; Jarvis), current public debates suggest that privacy continues to be a cherished value. But despite the eminent visibility of privacy issues in the media, its political salience is questionable. Concrete privacy-enhancing political measures are few and far between. Numerous initiatives have tried to politicize privacy issues and attempted to turn the widespread discontent with state (and corporate) surveillance practices into political protest mobilizations. But their efforts seem to have resulted only in isolated protests, not leading to a growing protest movement.

Why do we see this discrepancy that, on the one hand, citizens seem to strongly appreciate the value of privacy but that, on the other hand, state and corporate privacy intrusion usually remains without consequences? In the following article I will try to give at least a partial answer to this question. The article starts with a brief discussion of some of the findings of the literature on privacy activism. I will then present an overview over the most visible critical reactions to the revelations of the NSA surveillance practices and discuss whether or not privacy activists were able to use the window of opportunity the NSA scandal offered. I argue that the continuing weakness of privacy activists under the favorable conditions of the NSA scandal should be interpreted as a result of their coalition-building and framing strategies, which did not favor broad grassroots mobilization but a focus on existing institutions.

Privacy Activism

Privacy activism has received only scant scholarly attention. Early studies have addressed the protest mobilization for a boycott of the German census in the early 1980s as a social movement against surveillance and for data protection (Appel and

Hummel). More recently a handful of publications has looked into privacy activism triggered by the ever-growing data collection by private firms and state surveillance agencies on the internet (Bieber; Introna and Gibbons; Martin et al.). The most extensive study about privacy activism is certainly Colin Bennett's book about privacy advocates, in which he charts the groups and individual actors involved in privacy activism in North America, South America, Europe, and Australia. Bennett identifies several clusters of groups that address privacy issues as their main topic or from a civil liberties, a human rights, a consumer protection, and a digital rights perspective. Among those the consumer protection and digital rights groups are the most recent, usually founded in the late 1990s and early 2000s.

Bennett sees an increasing trend of group formation and political activity in the last twenty years, pointing to a growing political relevance of the issue. He argues that the political diversity of the groups suggests that privacy advocacy would not have a conventional ideology (58). But despite the growing number of groups, Bennett sees no signs of an emerging privacy, data protection, or anti-surveillance movement. For this he sees several reasons (209-15), notably that most of the groups lack the financial and personal resources to engage in broad public mobilizations, that privacy is a relatively diffuse and multi-dimensional issue, and that the existence of an established transnational advocacy network of privacy groups may actually hinder the development of a mass-based social movement (Keck and Sikkink 204). But, most importantly, he argues that the one thing that is missing in this policy field is a "Privacy Chernobyl," an "enormous privacy disaster that raises the issue to a new level of mass consciousness and political mobilization" (209-10).

Now, after Edward Snowden's revelations about the previously almost inconceivable surveillance practices of the NSA and its Five Eyes partner agencies in Australia, Canada, New Zealand, and the United Kingdom, it may be a good time to reconsider Bennett's evaluation. Is the NSA scandal the Privacy Chernobyl that has the potential to mobilize mass protests and to galvanize the various privacy advocacy groups into one privacy social movement? Some aspects support such a view:

- The scope of the surveillance practices revealed goes beyond what most commentators had expected. In comparison to the NSA's PRISM program through which it is collecting internet communication data from at least nine major US internet firms (Greenwald and MacAskill), or its DISHFIRE program that enables it to basically locate every mobile phone and read millions of SMS messages every day (Ball), issues addressed in earlier privacy campaigns appear almost minuscule. The same is true for British GCHQ's tapping of the mayor fiber-optic undersea cables in their "Tempora" program (Shubber).

- The global reach of the programs and the fact that the mass surveillance programs are not limited to a few authoritarian or unstable countries, might also create favorable conditions for a broad protest mobilization.
- Furthermore, the blatant breach of legal procedures could make these practices an easy target for protest mobilizations.

But despite all this there still seems to be no global privacy movement. While there certainly is some public interest in the issue, no movement comparable to the anti-nuclear or global justice movement has developed, mobilizing around issues of privacy, data-protection, and surveillance. Why don't we see such a movement? Why were privacy activists not able to seize the window of opportunity the NSA scandal seemed to offer? In order to understand why, even after a Privacy Chernobyl, no mass movement has developed, I will take a closer look at those civil society reactions and protest mobilizations that took place after Edward Snowden blew the whistle on the NSA's and others' surveillance practices in June 2013.

I will first analyze how the information about the surveillance practices was discussed at the international level within international political organizations, because these institutions are traditionally the main targets of transnational advocacy networks. The article then proceeds with an analysis of civil society activities and protest mobilizations that emerged in the first year after the scandal started to unfold.

Data and Methods

The following analysis is based on three bodies of data. First, information about demonstrations about privacy issues in the wake of the NSA scandal was collected by analyzing all news articles containing the terms "Snowden," "NSA," "demonstration," "rally," and "protest" taken from the Factiva English and German language international news collection, published between June 2013 and June 2014 (overall 324 articles).¹ Second, information about debates and activities in international organizations was collected directly on the organizations' web sites. And, finally, information about the framing of privacy issues by civil society organizations was collected by analyzing position papers and statements from those organizations most visible in the protest and/or judged as most important in the literature.

¹ The actual search term was the Boolean expression "(snowden OR NSA) AND (demonstration OR rally) AND protest*."

Debates and Activities in International Organizations

The exposed NSA surveillance practices did not only create discontent among privacy advocates in civil society organizations. The realization that the United States are able to monitor most other countries' telephone and internet communication was criticized harshly by several heads of government, most prominently Brazilian President Dilma Rousseff who cancelled her planned visit to the United States after press reports revealed that the NSA had tapped her phone (Borger). As a result of the global scope of the NSA surveillance practices two important international organizations have addressed privacy issues in the time after June 2013: the United Nations (in the General Assembly and in the UN Human Rights Council) and the European Parliament.

The United Nations General Assembly adopted in its 68th session on 18 December 2013 a draft resolution with the title "The Right to Privacy in the Digital Age." In the resolution the member states declare that the right to privacy would be important for the realization of the right to freedom of expression and voice their concern that mass surveillance and mass collection of personal data may have a negative impact "on the exercise and enjoyment of human rights" (UN General Assembly 2). In the following year this resolution was reaffirmed and updated. The UN resolution thus frames surveillance as a human rights problem. In line with this argumentation, it entrusts the UN Human Rights Council with more concrete activities and requests the UN Human Rights Council to prepare a report on the protection and promotion of the right to privacy in the context of mass surveillance and interception of digital communications.

This report was submitted in June 2014 and in its aftermath, on 26 March 2015, the UN Human Rights Council adopted a resolution and created the position of a new Special Rapporteur on the right to privacy, appointed for a period of three years to promote and protect this right (UN Human Rights Council).

The other international organization, which directly responded to the NSA scandal is the European Parliament. On 12 March 2014 it adopted a resolution "on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs" (EP), in which it denounces the NSA's and GCHQ's mass surveillance activities as espionage. Similar to the UN resolution, the EP resolution also starts with a reference to data protection and privacy as fundamental rights. But by choosing the term espionage, the EP then sets a different tone than the UN, which is also reflected in its condemnation of "the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information" (EP 11).

Apart from endangering individual (human) rights, the EP also criticizes the mass surveillance measures as unlawful under international and European law, and

warns that the massive blanket data collection without individual authorization by judges and courts would undermine core legal principles in democratic societies and interfere with democratic checks and balances (EP 11). The European Parliament thus responded to the NSA scandal with a – compared to the UN resolution – much more political resolution, calling “on the US authorities and the EU Member States, where this is not yet the case, to prohibit blanket mass surveillance activities” (EP 12) – a call that, not very surprisingly, so far remained without consequences.

Civil Society Activities

The UN and EP resolutions are clearly a sign that the revelations about the NSA’s and others’ mass surveillance practices created some turmoil at the highest political level, thus supporting the notion that this might indeed have been the Privacy Chernobyl with the potential to create a mass-based privacy or anti-surveillance movement.

How did civil society actors then respond to the publication of the Snowden files? Did the global scale of the surveillance trigger a similarly global protest mobilization? Which were the most central actors involved in privacy activism at this time?

Overall, large-scale civil society activities in response to the NSA scandal fall into two categories: petitions, open letters, and similar activities, on the one hand, and demonstrations, on the other hand. Only two activities, both from the first category, managed to develop a truly transnational reach. One attempt to mobilize for an internationally coordinated series of demonstrations failed for reasons of lacking participation.

Petitions and Open Letters

The origin of the most transnational mobilization predates Snowden’s revelations, but it gained significant momentum as a result of the NSA scandal. It is the concerted effort of a number of civil society organizations with a long record of privacy activism to develop a set of international principles on communications surveillance and human rights that could function as a guideline for national legislation and business practices. After two initial meetings in Brussels and Rio de Janeiro in October and December 2012, and led by the US and UK-based privacy advocacy groups Access, the Electronic Frontier Foundation (EFF), and Privacy International, an international group of human rights and digital rights experts drafted a set of thirteen principles. Under the heading “Necessary and Proportionate” these principles were published in July 2013, one month after the information about the NSA’s

and others' mass surveillance practices had been made public, on a dedicated website.² Officially launched at the UN Human Rights Council in Geneva in September 2013, these principles have been signed so far by 420 civil society organizations from almost every country in the world.

In their principles the privacy advocates demand that communications surveillance should require clear legal rules, should only be allowed for legitimate and important purposes. Moreover, surveillance measures should only be permitted if they are the only means to achieve the desired aim, and only if the measures are adequate to achieve this aim. Because communications surveillance is highly intrusive, it should only be allowed in connection with serious crimes, and only when ordered by a competent judicial authority following due process, including notification of those subjected to communication surveillance. Independent oversight should be established and guaranteed, the integrity of communication systems should not be compromised, international cooperation in surveillance activities should not break national laws, and illegitimate access to the collected data should not be possible.

This concerted effort of international privacy advocacy organizations has left at least some traces in the UN system, when the office of the United Nations High Commissioner for Human Rights repeatedly cited the principles in its 2014 report on *The Right to Privacy in the Digital Age* (UN Human Rights Council).

The largest civil society mobilization in terms of numbers of supporters was an open letter to the US Congress to enact legislation ensuring that blanket surveillance of the Internet activity and phone records of any person residing in the United States is prohibited by law. The campaign that, under the heading "Stop Watching Us," combined the open letter with a mobilization to a demonstration in Washington, D.C., on 26 October 2013, was organized and supported by about 85 organizations.³ Among them were privacy and digital rights advocacy organizations like EFF and Access, who already led the drafting of the Necessary and Proportionate principles, but also internet organizations (e.g. World Wide Web Foundation, Mozilla Foundation), some firms (e.g. reddit), and more traditional civil society organizations and parties (e.g. US Green Party, Greenpeace USA). According to the organizers more than 594,000 people have signed the open letter.⁴ No other civil society mobilization was able to gather similar numbers of supporters.

In Germany, it was also an open letter – this time to Chancellor Angela Merkel – that mobilized the highest number of supporters. Initiated by writer Julie Zeh, she and 58 other authors asked whether the German government was informed or even involved in the mass surveillance activities and demanded that Chancellor

² <https://en.necessaryandproportionate.org/text> (3 September 2015).

³ <https://optin.stopwatching.us> (3 September 2015).

⁴ <https://www.privacyinternational.org/?q=node/94> (3 September 2015).

Merkel should tell the truth about the surveillance program (Zeh). By September 2013 this open letter had gathered over 65,000 signatures.

This initiative was followed up by an international call from writers to respect citizens' rights to privacy and to create an international convention of digital rights. Initiated by Juli Zeh and six other writers from Germany, Denmark, Austria, the United Kingdom, and the United States, in December 2013 562 authors from over 80 countries, among them five laureates of the Nobel Prize for literature, launched an appeal in defense of civil liberties against surveillance (Zeh and Trojanow). In the text that was simultaneously published in thirty newspapers, they demanded "a right for all people to determine, as democratic citizens, to what extent their personal data may be legally collected, stored and processed, and by whom; to obtain information on where their data is stored and how it is being used; to obtain the deletion of their data if it has been illegally collected and stored."⁵ Their appeal received over 223,000 signatures from individual citizens on the petition website change.org.

Demonstrations

While the high number of signatories is an expression of heightened public concern about the NSA's surveillance practices, petitions are at the same time one of the weakest forms of protest. If Snowden's revelations really functioned as a Privacy Chernobyl, we should witness also increased participation in more demanding forms of protest, and especially large demonstrations or rallies. And, indeed, in the months after the publication of the first Snowden documents there were a couple of protest mobilizations that drew a significant number of participants. But overall these demonstrations remained exceptions. My search in international newspapers and activist websites revealed only two demonstrations attended by more than thousand participants: The "Freedom not Fear" (Freiheit statt Angst) demonstration on 7 September 2013 in Berlin and the "Stop Watching Us" demonstration on 26 October 2013 in Washington, D.C. For all other demonstrations either no participation numbers were given (this usually means that participation numbers were small), or protest participation ranged from several dozen up to a few hundred citizens.

The largest demonstration was the "Freedom not Fear" demonstration in Berlin, where 85 organizations had mobilized a protest against surveillance and for civil rights, data protection, and a free internet (Freiheit statt Angst). About 15,000 demonstrators participated in the march with speeches from several privacy and internet activists (Reißmann). The demonstration in 2013 in Berlin was the seventh in a series of demonstrations with the same title that started in 2006 and always ad-

⁵ <https://www.change.org/p/a-stand-for-democracy-in-the-digital-age-3> (3 September 2015).

dressed surveillance, data protection, and privacy issues. While being the largest demonstration in the aftermath of the NSA scandal, earlier “Freedom not Fear” demonstrations had actually drawn much higher numbers of participants. With a focus on the issue of data retention the demonstrations in 2008 and 2009 had mobilized more than 50,000 and 25,000 participants, respectively. Thus, compared to these earlier mobilizations, the demonstration in 2013 was actually not that big.

The largest demonstration in the United States was the “Stop Watching Us” protest on 26 October 2013 in Washington, D.C. About 100 organizations had formed a coalition to mobilize for this demonstration that accompanied the above mentioned open letter to the US Congress with the same name. But despite the large number of organizations supporting the call for the demonstration, only about 2,000 participants attended the protest (Gorman). There seems to be a stark difference between the willingness to participate in low-effort ‘clicktivism,’ on the one hand, and even moderately more demanding forms of political protest, on the other hand. This became even more apparent in the wake of the mobilization of an internationally coordinated protest event under the heading “The Day We Fight Back.”⁶ The organizers, among them long-term privacy and civil rights advocacy organizations like Electronic Frontier Foundation (EFF) or the American Civil Liberties Union (ACLU), claim that on the day of action on 11 February 2014 about 185,000 Americans did send emails to their representatives and that the campaign website was shared more than 420,000 times on Facebook, but none of the 24 announced events in 15 countries drew more than a couple of hundred participants.⁷

Overall, thus, this brief analysis of protests that developed after Edward Snowden’s revelations about the NSA’s all-encompassing spying activities shows that, first, despite the global reach of the surveillance operations, significant protest really only developed in the United States and in Germany. In some other countries, isolated small-scale protests happened, but only in the United States and Germany did civil society mobilizations reach a size so that national news sources started to report them. This stands in surprising contrast to the truly international composition of the advocacy network of organizations engaged in privacy activism and mobilizing of various protests events during this time. Second, large numbers of citizens voiced their concerns through low-effort online tools, but only few were willing to participate in more traditional and more demanding forms of protest in the form of demonstrations or rallies.

In light of these preliminary results, we have to conclude that either the public exposure of current state surveillance practices did not constitute a Privacy Cher-

⁶ <https://thedaywefightback.org> (9 September 2015).

⁷ Only eleven out of the twenty-four events were announced as protests or demonstrations. The others were speaking events, cryptoparties, or other events that were from the outset aimed at fewer participants.

nobyl because it did not indicate a similar level of system failure or because the perceived consequences were less severe. Or it could be that the reason for the missing protest activities should be sought not in the characteristics of the event but in the mobilization strategies of the privacy activism groups. In the final part of this article, I will try to investigate this second line of argument.

Actors and Frames

Taking a lead from the literature on social movements, I will analyze to which degree the protest mobilizations that followed Edward Snowden's revelations about the encompassing surveillance practices meet the criteria that are usually associated with successful – not mainly in terms of policy outcomes but in terms of sizeable and sustained protest – social movements: densely connected actor networks (Diani) and framing strategies that motivate individuals to participate in demonstrations and other forms of protest (Benford and Snow).

The Network of Actors

Why were privacy advocacy groups not able to convince more people to participate in demonstrations against surveillance or for privacy? One possible explanation might be that groups were not diverse enough in terms of provenance, issues addressed, or ideology. In addition, it might be that the groups did not cooperate enough with each other.

To test the plausibility of these options, I analyze the network of organizations involved in the Necessary and Proportionate mobilization, the mobilization that was supported by the largest number of organizations. Because for none of the mobilizations data about actual cooperation relationships between participating organizations and individuals is available, I resort for this analysis to the cooperation links between organizations as manifested in the hyperlink network between their websites. Based on the literature on online and offline cooperation in protest mobilizations, this can serve as a fairly reliable proxy, because organizations with close offline cooperation relationships usually also tend to exchange links on their websites (Van Aelst and Walgrave; Badouard and Monnoyer-Smith).

Fig. 1 represents the interlink network of the organizations involved in the Necessary and Proportionate mobilization. Organizations are color coded according to their main policy field, with traditional civil- and human rights organizations appearing as yellow nodes, organizations mainly concerned with freedom of expression (incl. freedom of press) in red, privacy advocacy organizations in green, internet/digital rights organizations in blue, and other organizations in white.

The network data for this graph was collected by feeding the URLs of the websites of all organizations who signed the Necessary and Proportionate declaration into the link analysis tool “Issue Crawler” (Rogers). The program then returns the network of all hyperlinks connecting the organizations. Hyperlinks are directed relations going from the originating to the target website. They can be interpreted as statements of relevance or importance. If an organization creates a hyperlink to another organization’s website, this is a statement that the receiving organization is deemed important by the sending organization. The number of incoming ties, measured as a node’s indegree, can thus be interpreted as an expression of relative status in the network of organizations that constitute the network. The number of outgoing ties cannot be interpreted in a similar way. It merely reflects an organization’s website design policy.

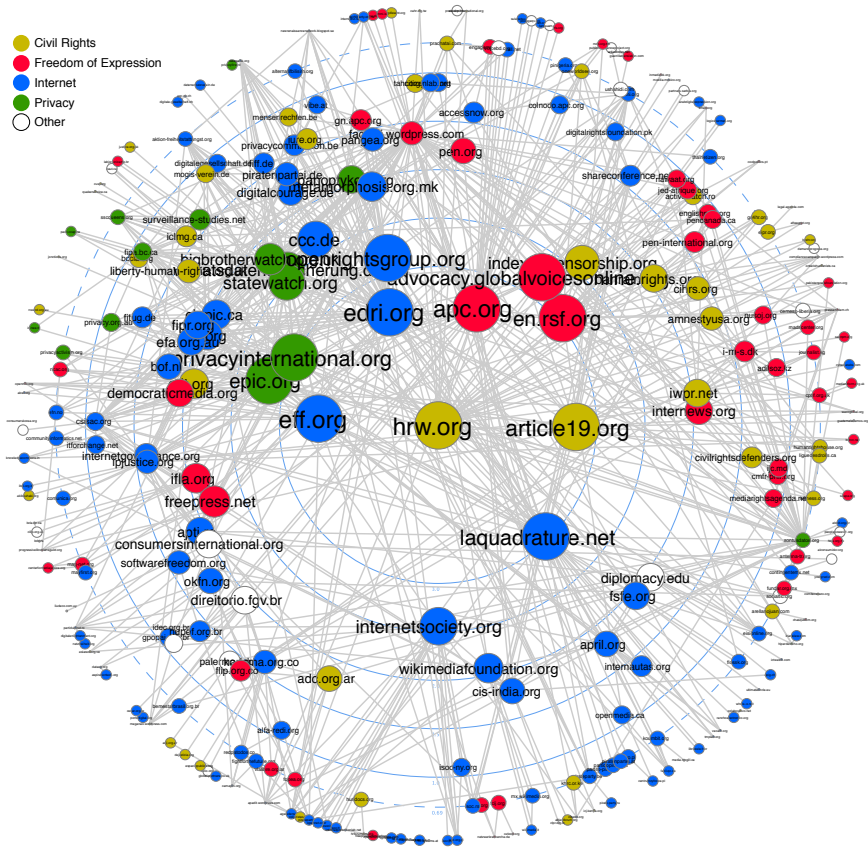


Fig. 1: Interlink network Necessary and Proportionate.

The graph of the interlink network visualizes several aspects. First, almost all nodes (269 of 279 for which reliable website information could be retrieved) form one giant component, that is they are all at least indirectly connected with each other. Second, the hyperlink network among the organizations who signed the Necessary and Proportionate principles is not particularly dense. About 2% of all possible links are realized, on average organizations are linked with 6.4 other organizations. Third, the organizations with the highest indegree centrality values are organizations well known in the literature about privacy activism. This confirms the assumption that hyperlink networks among civil society organizations are correlated to offline relationships between them. Fourth, the most central organizations are diverse in terms of their main policy focus, and most of them are also strongly linked to each other. The most central organizations comprise dedicated privacy advocacy organizations, more general civil right organizations, organizations that address issues of freedom of the press and freedom of expression, and internet/digital rights organizations. The network also shows weak signs of preferential attachment, i.e. organizations tend to be linked more closely to organizations from the same policy field. But overall the diversity of thematic fields especially in the network core should be interpreted as a favorable asset of the network as it theoretically translates into the ability to mobilize a broader constituency compared to a network of groups coming from one policy field only.

In sum, the characteristics of the interlink network among the organizations involved in the Necessary and Proportionate mobilization provide no clues for the apparent inability of the organizations to mobilize large scale protests in response to the Snowden revelations. On the contrary: based on the interlink network one would have expected a much stronger contentious political response.

Framing Strategies

A closer look at the actors thus rather exacerbates the puzzle why the Snowden revelations did not lead to a privacy or anti-surveillance protest movement. I therefore finally turn to the privacy advocates' framing strategies. Did they frame the issue in ways that hindered the emergence of large scale protests? This analysis is based on a content analysis of documents published by ten organizations which have high indegree centrality values in the interlink network detailed above and which have been involved in several mobilizations after Snowden's NSA documents were published. Following an established practice in the analysis of framing strategies in social movements (Benford and Snow; Gerhards and Rucht), for each organization one document which explicitly refers to the current debate about state surveillance practices was chosen. In these documents all statements related to diagnostic frame – those parts of an argumentation that establish the problem and name those responsible for it – and all statements related to the prognostic frame –

those arguments that detail what should be done – were annotated using the qualitative data analysis package RQDA (Huang).

In their documents the most central actors in the interlink network employ four general frames, each consisting of a diagnostic and a prognostic sub-frame, in their attempts to mobilize protest against the current surveillance practices and for data protection and privacy. These four frames are a civil rights frame, a general data protection frame, a security agencies frame, and a surveillance technology frame.

The Civil Rights Frame

The most general frame used by the privacy advocates (for example by the Association for Progressive Communications [APC], Reporters Sans Frontières [RSF], the Umbrella organization European Digital Rights [EDRi], Human Rights Watch [HRW], or Privacy International) is the civil rights frame. The *diagnostic frame* of the civil rights frame starts from the general claim that privacy is a fundamental human right, and it is central to the maintenance of democratic societies and human dignity. Privacy reinforces other rights, such as freedom of expression and information, and freedom of association. The problem now is that the limited scope of privacy protection for national citizens and the more or less complete lack of privacy protection for foreign citizens invalidates these rights.

In their *prognostic framing* the organizations argue that people should be able to communicate free of the threat of surveillance and interception and that all security and surveillance measures should be necessary, proportionate, and implemented based on solid evidence. In order to secure privacy, “informational self-determination” should be regarded as a fundamental democratic right.

The General Data Protection Frame

The general data protection frame, employed for example by EDRi or APC is similar to the civil rights frame but focuses less on rights and more on practices. It starts from the problem (*diagnostic frame*) that citizens are constantly watched and lose trust in administrations and businesses. This would be damaging for democracy and for business. The argument is thus that governments and companies are undermining the trust they depend on.

In the *prognostic frame* of the general data protection frame the organizations claim that safeguards would be needed. Citizens should provide explicit, specific, and freely-given consent before their personal data can be processed. Privacy protection should become the default, and states should access data only according to mutual legal assistance treaties that respect international human rights standards. Security and surveillance measures should only be allowed when they are necessary, proportionate, and implemented based on solid evidence. The guiding princi-

ple should be that people know who stores what data about them. This frame thus argues in favor of a general data protection policy and addresses security agencies as one actor among others.

The Security Agencies Frame

The main perpetrators of mass surveillance are directly addressed in the third general frame, put forward for example by Privacy International, RSF, the Fundamental Rights Experts Group (FREE), the Chaos Computer Club (CCC), and again by EDRi. In their *diagnostic framing*, the organizations argue that today intelligence agencies would be more powerful than ever, and that their activities have been outside democratic oversight and clear legal frameworks. In a stronger version, the argumentation goes that the current global surveillance practices would be fundamentally opposed to the rule of law and to the well-established international human right to privacy, and that current surveillance practices would be a blatant and systematic disregard of human rights.

The *prognostic framing* then focuses on curbing the security agencies' competencies. More concretely, parliaments and the public should become enabled to effectively control the security agencies with the aim of restoring trust through transparency and by bringing the intelligence agencies under the rule of law. In addition, a competent, independent, and impartial judicial authority would be needed to oversee and control the surveillance activities.

Whereas the general data protection frame aims at creating a general privacy and data-protection friendly environment, the security agencies' frame specifically wants to limit the competencies of these organizations.

Surveillance Technology Frame

Finally, a fourth frame that for example the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF), and the CCC are using in their documents is less focused on states, institutions, or organizations, but on technologies.

The surveillance technology frame claims in its *diagnostic framing* that the internet facilitates spying and surveillance because security aspects have been neglected when digital communication technologies were designed and implemented. The organizations using the surveillance technology frame argue that one core problem is that so-called metadata often reveal as much or even more about an individual than the content of the digital communication. Mass surveillance then has a chilling effect. Some organizations even argue that the NSA has corrupted the internet.

The *prognostic framing* also focuses on technological and procedural fixes, namely that a paradigm shift towards default end-to-end-security would be necessary, and that national and international laws would have to catch up with the evolving need for privacy that comes with new technology. The development of privacy-protecting technologies is seen as the appropriate answer to the current mass surveillance practices.

These four general frames have not been mutually exclusive. Some organizations have combined two or even three of the frames in their argumentation (e.g. EDRi), others rely only on one specific frame. Nevertheless, the frame analysis of the argumentation strategies of the most central actors in the civil society mobilization against mass surveillance and for privacy and data protection shows no signs of one emerging unifying master frame that would connect and integrate the different lines of argumentation. Despite the many connections among the organizations, they do not share a common understanding about the problems mass surveillance generates and about the political and/or technical solutions to solve these problems.

Moreover, on a substantial level, the *diagnostic frames* mainly focus on the indirect harm of mass surveillance. Instead of arguing that mass surveillance would directly create harm for citizens, they argue that citizens may alter their behavior in light of the surveillance practices and this would then have negative effects on the functioning of democratic societies and institutions. The surveillance practices are portrayed as creating an environment detrimental to the free expression of one's views and convictions. Overall, the diagnostic framing creates only a weak "injustice frame," which is an emotional or, as Gamson calls it, "hot" cognition (32) that can convince large numbers of citizens that immediate and consequential action is necessary, and which in other mobilizations often builds the base of a movement's discursive strategies.

The *prognostic framing* focuses, on the one hand, on technological solutions and, on the other hand, on (international) legal action. From a mobilization perspective, the problem with the technical solutions is the unclear addressee. Who should develop and implement these technical solutions – especially in a situation where the necessary technical knowledge seems to be very advanced and specialized? Putting one's hopes on legal action and thus on national parliaments also seems questionable when the rationale at the same time claims that parliaments have generally been weak actors in terms of controlling and overseeing surveillance. How should weak parliaments be able to pass strong legislation?

Conclusion

After Edward Snowden's disclosures had generated "unprecedented public interest in surveillance in many countries around the world" (Lyon 9), many commentators expected the emergence of widespread protests against these mass surveillance practices and for privacy and data protection. And indeed, the high salience of the issue, the favorable political opportunity structure, and the already existing network of information exchange and cooperation among privacy advocacy organizations would have pointed to the likely emergence of a protest movement on this issue. But as I have shown, this expectation was premature. Several online campaigns were supported by more than half a million citizens, but even slightly more demanding forms of protest like demonstrations mobilized – with one notable exception – only few participants.

Based on an analysis of the most visible contentious mobilizations about surveillance and privacy and an assessment of the argumentations used in the most central organizations' statements, an explanation for the nonappearance of a privacy social movement should be sought in the framing strategies. The privacy advocates framed the issue as a problem requiring either a technical fix or legal action from international organizations and national parliaments. They thus essentially offered a reformist framing with only limited mobilization potential.

The argumentation put forward by core privacy organizations offered frame bridges to traditional civil and human rights advocacy organizations who joined the protest mobilizations. With them they also shared a preference for low-conflict forms of action addressing mainly international organizations. Frame bridging to other knowledge society conflicts about intellectual property rights, net neutrality, and other digital rights (Haunss) could not be observed even though the actor network comprises several organizations active in these policy fields.

Overall, the analysis of contentious mobilizations after Snowden's revelations shows that a Privacy Chernobyl is not enough to start an anti-surveillance or pro-privacy social movement. Existing advocacy networks tried to seize the opportunity to mobilize for large protest demonstrations, but their framing remained focused on their traditional allies in international organizations and expert communities concerned with issues of human and civil rights.

A social movement needs a mobilized network, a collective identity, and a master frame (Melucci; della Porta and Diani). The network of organizations active in privacy activism, civil and human rights, internet politics, and digital rights might be a solid base for a privacy movement. What is missing is a master frame that would provide groups and individuals with different backgrounds, a shared interpretation of the problem at hand, and the desired solution, as well as a strong incentive to act. This in turn would be a precondition for the development of a collective identity defining the 'we' of a collective actor and its field of action, which

– in the case of a social movement – is never limited to hallways of international organizations and national parliaments.

Works Cited

- Appel, Roland, and Dieter Hummel. "Die Republik nach der Volkszählung." *Die neue Sicherheit: Vom Notstand zur sozialen Kontrolle*. Ed. Roland Appel, Dieter Hummel, and Wolfgang Hippe. Köln: Kölner Volksblatt-Verlag, 1988. 9-37. Print.
- Badouard, Romain, and Laurence Monnoyer-Smith. "Hyperlinks as Political Resources: The European Commission Confronted with Online Activism." *Policy & Internet* 5.1 (2013): 101-17. Print.
- Ball, James. "NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep." *The Guardian* 16 January 2014. Print.
- Benford, Robert D., and David A. Snow. "Framing Processes and Social Movements: An Overview and Assessment." *Annual Review of Sociology* 26.1 (2000): 611-39. Print.
- Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press, 2008. Print.
- Bieber, Christoph. "Datenschutz als politisches Thema – von der Volkszählung zur Piratenpartei." *Datenschutz: Grundlagen, Entwicklungen und Kontroversen*. Ed. Jan-Hinrik Schmidt and Thilo Weichert. Bonn: Bundeszentrale für politische Bildung, 2012. 34-44. Print.
- Borger, Julian. "Brazilian President: US Surveillance a 'Breach of International Law.'" *The Guardian* 24 September 2013. Print.
- della Porta, Donatella, and Mario Diani. *Social Movements: An Introduction*. Oxford: Blackwell, 1999. Print.
- Diani, Mario. *The Cement of Civil Society: Studying Networks in Localities*. Cambridge: Cambridge University Press, 2015. Print.
- EP. *European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI))*. Strasbourg: European Parliament, 2014. Print.
- Freiheit statt Angst. "Aufruf zur Großdemonstration 'Freiheit statt Angst' 2013 in Berlin." *blog.freiheitstattangst.de* 7 September 2013. Web. 3 September 2015.
- Gamson, William A. *Talking Politics*. Cambridge: Cambridge University Press, 1992. Print.

- Gerhards, Jürgen, and Dieter Rucht. "Mesomobilization: Organizing and Framing in Two Protest Campaigns in West Germany." *American Journal of Sociology* 98.3 (1992): 555-96. Print.
- Gorman, Ryan. "Protesters Swarm Capitol Hill on 12th Anniversary of Data Collection Laws Authorizing NSA Spying." *MailOnline (The Daily Mail)* 27 October 2013. Web. 3 September 2015.
- Greenwald, Glenn, and Ewen MacAskill. "NSA Prism Program Taps in to User Data of Apple, Google and Others." *The Guardian* 7 June 2013. Print.
- Haunss, Sebastian. *Conflicts in the Knowledge Society: The Contentious Politics of Intellectual Property*. Cambridge: Cambridge University Press, 2013. Print. Heller, Christian. *Post-Privacy: Prima leben ohne Privatsphäre*. München: C.H. Beck, 2011. Print.
- Huang, Ronggui. *RQDA: R-based Qualitative Data Analysis*. N.p., 2010. Web. Introna, Lucas D., and Amy Gibbons. "Networks and Resistance: Investigating Online Advocacy Networks as a Modality for Resisting State Surveillance." *Surveillance & Society* 6.3 (2009): 233-58. Print.
- Jarvis, Jeff. *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*. New York: Simon & Schuster, 2011. Print.
- Keck, Margaret E., and Kathryn Sikkink. *Activists Beyond Borders*. Ithaca, NY: Cornell University Press, 1998. Print.
- Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1.2 (2014): 1-13. Print.
- Martin, Aaron K., Rosamunde E. van Brakel, and Daniel J. Bernhard. "Understanding Resistance to Digital Surveillance: Towards a Multi-disciplinary, Multi-actor Framework." *Surveillance & Society* 6.3 (2009): 213-32. Print.
- Melucci, Alberto. *Challenging Codes: Collective Action in the Information Age*. Cambridge: Cambridge University Press, 1996. Print.
- Reißmann, Ole. "NSA-Protest in Berlin: Freiheit unterm Alu-Hut." *Spiegel Online* 7 September 2013. Web. 3 September 2015.
- Rogers, Richard. "Mapping Public Web Space with the Issuecrawler." *Digital Cognitive Technologies: Epistemology and Knowledge Society*. Ed. Claire Brossard and Bernard Reber. London: Wiley, 2010. 115-26. Print.
- Shubber, Kadhim. "A Simple Guide to GCHQ's Internet Surveillance Programme Tempora." *Wired UK* 24 June 2013. Print.
- UN General Assembly. *The Right to Privacy in the Digital Age*. New York, NY: United Nations, 2013. Print.
- UN Human Rights Council. *The Right to Privacy in the Digital Age*. New York, NY: United Nations, 2015. Print.
- . *The Right to Privacy in the Digital Age*. New York, NY: United Nations, 2014. Print.

- Van Aelst, Peter, and Stefaan Walgrave. "New Media, New Movements? The Role of the Internet in Shaping the 'Anti-Globalization' Movement." *Information, Communication & Society* 5.4 (2002): 465-93. Print.
- Zeh, Juli. "Deutschland ist ein Überwachungsstaat: Offener Brief an Angela Merkel." *Frankfurter Allgemeine Zeitung* 25 July 2013. Print.
- , and Ilija Trojanow. "Demokratie im digitalen Zeitalter: Der Aufruf der Schriftsteller." *Frankfurter Allgemeine Zeitung* 10 December 2013. Print.