Do-It-Yourself Data Protection—Empowerment or Burden?

Tobias Matzner, Philipp K. Masur, Carsten Ochs and Thilo von Pape

Abstract Data protection by individual citizens, here labeled do-it-yourself (DIY) data protection, is often considered as an important part of comprehensive data protection. Particularly in the wake of diagnosing the so called "privacy paradox", fostering DIY privacy protection and providing the respective tools is seen both as important policy aim and as a developing market. Individuals are meant to be empowered in a world where an increasing amount of actors is interested in their data. We analyze the preconditions of this view empirically and normatively: Thus, we ask (1) Can individuals protect data efficiently; and (2) Should individuals be responsible for data protection. We argue that both for pragmatic and normative reasons, a wider social perspective on data protection is required. The paper is concluded by providing a short outlook how these results could be taken up in data protection practices.

Keywords Do-it-yourself data protection · Data protection · Responsibilization · Data protection advocates · Data protection practices · Representative study · Privacy paradigm

T. Matzner (✉)
Universität Tübingen, Internationales Zentrum für Ethik in den Wissenschaften,
Wilhelmstr. 19, 72074 Tübingen, Germany
e-mail: tobias.matzner@uni-tuebingen.de

P.K. Masur · T. von Pape
Universität Hohenheim Lehrstuhl Für Medienpsychologie (540 F), 70599 Stuttgart
(Hohenheim), Germany
e-mail: philipp.masur@uni-hohenheim.de

T. von Pape
e-mail: thilo.vonpape@uni-hohenheim.de

C. Ochs
Universität Kassel Fachbereich 05 Soziologische Theorie,
Nora-Platiel-Str. 5, 34109 Kassel, Germany
e-mail: carsten.ochs@uni-kassel.de

S. Gutwirth et al. (eds.), *Data Protection on the Move*,
Law, Governance and Technology Series 24, DOI 10.1007/978-94-017-7376-8_11

1 Introduction

In current debates, do-it-yourself (DIY) data protection is often conceived as an important element of comprehensive data protection. In particular after the revelations of Edward Snowden and the ensuing distrust in states or legal frameworks, prominent individuals (among them Snowden himself) and NGOs have advocated DIY data protection as the main and most immediate way to protect citizens' data. Here, the term DIY data protection[1] is intended to encompass all measures taken by *individual persons* to protect their data. This includes the use of cryptography and anonymization tools, browser plugins that manage cookies or block tracking and other tools used to minimize data collection. We also include tools which are meant to increase the transparency of data processing, e.g. plugins like Lightbeam which visualize tracking. Apart from tools, data minimization strategies are considered as DIY data protection practices. These include using fake data and profiles, a very conscious and selective provision of data, and not using particular services and technologies at all. There are also some legal actions like requesting the deletion of personal data that can be taken by individuals. These approaches are based on the premise that increasing knowledge about data collection practices and the possible insights that can be derived from data leads to better individual judgments and decisions. Thus fostering knowledge and awareness concerning data is seen as one important contribution to DIY data protection.

In this chapter, we want to take a step back from this premise and question the overall concept of DIY data protection from an empirical and normative perspective: to what extent *can* and *should* our response to data protection problems center on the individual user?

Before responding to these questions, we want to put them into perspective by reconsidering a long lasting debate about another information communication technology (ICT)-related concern: the "digital divide". This discussion still suffers from what Rogers called an "individual-blame-bias"[2]: instead of blaming structural causes for inequalities related to ICT use, the non-adoption of relevant information technology is often attributed to deficits of those "laggards" and "information have-nots"[3] who are on the "wrong" side of the divide because they

[1]The term "DIY data protection" was conceived as translation of the German "Selbstdatenschutz", which literally translates as self-data-protection. Thus, the usual connotations of DIY as improvised or alternative to a commercial product are not necessarily intended; the connotations of independence and self-reliance, however, are. The results presented in this article build on a German whitepaper concerning "Selbstdatenschutz" issued by the research project "Privacy Forum" which can be found here: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (accessed 06.03.2015).

[2]Everett M. Rogers, *Diffusion on Innovations* (New York: Free Press, 2005), 118.

[3]National Telecommunications and Information Administration (NTIA), *Falling Through the Net: A Survey of the 'Have-nots' in Rural and Urban America* (Washington, DC: US Department of Commerce), assessed March 10, 2015. http://www.ntia.doc.gov/ntiahome/fallingthru.html.

lack knowledge, social status, or resources.[4] In a similar vein, the deficits in data protection and a lack of implementation today, are often explained through the users' rational and behavioral deficits. They are characterized as a paradox between the users' concerns and attitudes favoring restrictive use of data on the one hand and a very permissive actual use on the other.[5] Failing to see the larger, structural reasons behind individual lacks in privacy protection, this perspective also does not attribute responsibility to the government as the actor who might be able to address structural problems. Finally, even some of those advocates who do blame the government and Internet Service Providers eventually put pressure on the users to take the protection of their privacy into their own hands. For cyber-libertarians such as John Berry Barlow, it would be paradoxical to confide the protection of privacy to the government in principle because this task would go against any government's interest of controlling its citizens.[6]

In consequence, the most discussed explanations focus on deficits of the users or human nature in general: the users are labeled as lacking literacy with respect to privacy,[7] as corruptible by questionable gratifications such as negligible financial rewards or convenience,[8] and as hypocrite to the extent that their apparent concern for privacy may be explained through a social desirability response bias.[9] In short, the problems we perceive with data protection are often presented as simple "user errors". Correcting these errors by fostering DIY data protection is then considered as empowering users. However, as we will argue below, more and more problems with data protection remain, even when users behave through rational and educated decisions. There seems to remain a problem, which should rather be described as a privacy dilemma[10] than a paradox.

This leads us back to the questions we want to answer in the next sections: (1) Can we, the users, actually protect our data? How probable is the emergence of

[4]For profound critiques of the term "digital divide" and its applications in public discourse, see Neil Selwyn, "Reconsidering political and popular understandings of the digital divide," *New Media & Society* 6 (2004): 341–362, and David J. Gunkel, "Second Thoughts: Towards a Critique of the Digital Divide," *New Media & Society* 5 (2003): 499–522.

[5]Susan B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday* 11 (2006), accessed March 4, 2015, doi:10.5210/fm.v11i9.1394.

[6]Lincoln Dahlberg, "Cyber-Libertarianism 2.0: a discourse theory/ critical political economy examination. Cultural Politics 6, no. 3 (2010), doi: 10.2752/175174310X12750685679753: 331–356.

[7]Yong J. Park, "Digital Literacy and Privacy Behavior Online," *Communication Research* 40, no. 2 (2013).

[8]Alessandro Acquisti, Leslie K. John and George Loewenstein. "What is privacy worth?," *The Journal of Legal Studies* 42 *(*2013): 249–274.

[9]e.g., Miriam J. Metzger, "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication* 12 (2007): 351.

[10]Petter Bae Brandtzæg, Marika Lüders, and Jan Håvard Skjetne, "Too many Facebook 'friends'? Content sharing and sociability versus the need for privacy in social network sites," *Intl. Journal of Human–Computer Interaction* 26 (2010): 1006–1030.

DIY DP practices as a mass phenomenon? Can users enable themselves—or be enabled—up to a point where they can take the best decisions in their own interest and can this solve the problem of data protection or only reveal the true dilemmas lying beyond the users' field of action? And—notwithstanding these empirical questions—(2) should we, the users, have to protect data ourselves? Is it normatively desirable to choose the individual user as the main responsible actor to improve the state of data protection?

2 DIY-Data Protection—Can We Do It?

In this section we will deal with the question of how probable the emergence of DIY data protection practices as a mass phenomenon may be in empirical terms. To do so, we will cover three aspects of DIY data protection practices: the question to what extent it is possible for individuals to cultivate such practices (Sect. 2.1); the competing needs and aims which must be taken into account as the context of these practices (Sect. 2.2), and finally the question of DIY data protection practices, as collective activity, being entangled in specific socio-political constellations (Sect. 2.3).

2.1 The Individual Faced with the (Im)possibility of DIY Data Protection

Protecting personal data in online environments is a difficult task for individual users. The exponential growth of "smart" technologies, which quickly move into cultural mainstream, has led to a socio-technological environment in which manifold forms of tracking, data mining, and profiling have emerged.[11] As these data collection practices become more complex and elusive, potential negative consequences of information and communication technology usage are not readily perceivable. Awareness of data collection practices however is a crucial precondition for users to implement DIY data protection practices.[12] Negative outcomes of these practices are mostly not visible or sensible in the daily use of ICT. Grasping the complexities and flows of personal information in the web consequently becomes a rather difficult task, even for interested users or experts.

[11]Georgia Skouma and Laura Léonard, "On-Line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection," in *Reforming European Data Protection Law*, ed. Serge Gutwirth, Ronald Leenes, and Paul de Hert (Dordrecht: Springer, 2015), 35–62.

[12]George R. Milne and Andrew J. Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy & Marketing* 19, no. 2 (2000): 238–49.

Moreover, in online environments, human communication traverses spheres that are private, public, and social.[13] Previously separated media platforms converge and formerly distinct barriers are blurred. Consequently, data disclosed to one provider might be used by another and resold to third parties. Information communicated to one or several users might be reused, shared or misused by others. Potential threats to informational privacy thus arise from different contexts and dimensions. Furthermore, violations may in particular occur because boundaries of formerly distinct contexts and dimensions become increasingly blurred. Consequently, DIY data protection becomes an even bigger challenge as there is not one globally applicable data protection strategy. In fact, to ensure comprehensive protection against most potential privacy threats, a number of diverse and differently demanding strategies have to be implemented. For most cases, the implementation of a certain practice might require another one, which in turn necessitates another one and so on. For example, if a user wishes to be unrecognizable for online service providers, it is not sufficient to merely opt out from these services. The user furthermore needs to use anonymization tools every time he or she uses the internet and install plugins which hinder online service providers from tracking their surfing activities. Again, the understanding and evaluation of these practices both from a structural and technological perspective demands high competence from individual users.

To categorize DIY data protection practices, it seems fruitful to differentiate measures taken by the individual on a number of different levels. A first distinction refers to the question against whom or what a specific data protection strategy is directed. When sharing data in online environments, several actors with different interests and resources are involved in processing and using the data. On one hand, internet users want to protect their personal data against misuse by other users, but on the other hand, they also want to protect themselves against data collection by companies and institutions. Raynes-Goldie[14] defines the former as *social privacy* and the latter as *institutional privacy*. The protection of social privacy is at least partly realizable by using privacy settings (e.g., restricting visibility, separating audiences, managing disclosures). However, studies have also shown that even social privacy requires different approaches. De Wolf and colleagues for example found that it is not sufficient to imply individual privacy management practices, but also group privacy management practices.[15] To gain an optimal level of social privacy thus involves also the negotiation of common privacy rules. Controlling institutional privacy requires even more sophisticated measures and more general

[13]Zizi A. Papcharissi, *A Private Sphere: Democracy in a Digital Age* (Cambridge: Polity Press, 2010).

[14]Katie Raynes-Goldie, "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook," *First Monday* 15, no. 1 (2010).

[15]Ralf De Wolf, Koen Willaert, and Jo Pierson, "Managing privacy boundaries together: Exploring individual and group privacy management strategies on Facebook," *Computers in Human Behavior* 35 (2014).

approaches such as general data parsimony,[16,17] anonymization, pseudonymization and encryption.

Another differentiation refers to passive and active DIY data protection practices. Passive strategies include all strategies relying on withdrawal (opting-out) or data parsimony. As such, they involve the general decision to share or not to share personal information which might be reflected with regard to individual privacy preferences and situational needs (cf. Sect. 2.2). These strategies includes applying general rules of thumb in decisions on sharing, but also the constant monitoring and regulation of disclosures. Active strategies, on the other hand, encompass the use of privacy-enhancing-technologies and taking legal actions. As such, they serve to build a protected sphere, in which users can perform their selves without worrying about potential privacy threats.

DIY data protection practices can further be differentiated into preventive and corrective measures.[18] Whereas most strategies mentioned above can be referred to as preventive measures, there are also a number of actions that users take after a privacy violation has occurred. Among others, these include passive measures such as deleting previously shared content, unlinking or untagging[19] as well as active measures such as taking legal actions (e.g., asking online service providers not to share personal data with other companies or to delete all information about oneself).

Recent studies in the fields of media psychology and communication sciences have examined a number of different DIY data protection practices in the context of social web use and in particular on social network sites. The findings from these studies suggest that users do engage in DIY data protection to prevent attacks on their *social privacy*. These attacks may include inappropriate friend requests,[20] unwanted forwarding or sharing of personal information by other users, discrimination or exposition of sensitive information in public realms. Based on these studies, it can be said that a considerable number of users implement preventive strategies such as faking user names,[21,22,23] using privacy settings to separate

[16]Airi Lampinen et al., "We're in It Together: Interpersonal Management of Disclosure in Social Network Sercives," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, USA: ACM, 2011), 3217–3226.

[17]Philipp K. Masur and Michael Scharkow, "Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies", (in prep).

[18]Lampinen et al., "We're in It Together: Interpersonal Management of Disclosure in Social Network Services." .

[19]Ibid.

[20]Raynes-Goldie, "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook.".

[21]Zeynep Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society* 28, no. 1 (2008): 20–36.

[22]Tobias Dienlin and Sabine Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology* (2014).

[23]Bernard Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* 15, no. 1 (2009): 83–108.

audiences,[24,25] befriending only trusted people[26] and generally restricting the visibility of profile information.[27,28] Furthermore, users also regulate and constantly monitor their disclosing behavior. A study by Masur and Scharkow[29] found that most user actively manage their disclosure by generally sharing less information that they individually perceive as private. Users generally show this type of behavioral pattern, although it is more pronounced in one-to-many communication situations than in one-to-one communications. Results from different studies furthermore revealed that users seem to be more willing to implement specific privacy protection strategies after negative experiences with social privacy violations.[30,31]

Whereas many studies suggest that users seem to safeguard their social privacy at least partially, only a few studies have examined DIY data protection practices in the context of *institutional privacy*. Current societal debates often proclaim that users do not engage in data protection and consequently demand more literacy. In a recent study, Trepte, Masur and Teutsch examined the implementation of DIY data protection practices in the context of institutional privacy.[32] The analysis is based on an online-survey with a representative sample of German internet users ($N = 1932$). The findings revealed that internet users generally do implement some strategies. However, some practices are more widespread than others (see Table 1). In general, a third of the participants engage in passive data protection strategies such as refraining from registering for certain online services (75 %) or stopping to use certain websites (65 %) due to privacy concerns. Also 63 % reported that they have refrained from registering for certain online services after

[24]Eden Litt, "Understanding social network site users' privacy tool use," *Computers in Human Behavior* 29, no. 4 (2013): 1649–1656.

[25]Jessica Vitak, "The Impact of Context Collapse and Privacy on Social Network Site Disclosures," *Journal of Broadcasting & Electronic Media* 56, no. 4 (2012): 451–470.

[26]Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences.".

[27]Dienlin and Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors.".

[28]Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences.".

[29]Masur and Scharkow, "Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies".

[30]Sabine Trepte, Tobias Dienlin, and Leonard Reinecke, "Risky Behaviors: How Online Experiences Influence Privacy Behaviors," in *Von Der Gutenberg-Galaxis Zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy. Surveying Old and New Frontiers after 50 Years of DGPuK*, ed. Birgit Stark, Oliver Quiring, and Nikolaus Jackob (Wiesbaden: UVK, 2014), 225–246.

[31]Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences.".

[32]Philipp K. Masur, Doris Teutsch, and Sabine Trepte, "*Entwicklung der Online-Privatheitskompetenz-Skala*" (in prep).

Table 1 Do-it-yourself data protection practices in the German population (in %)

	Overall	Men	Women	14–19 years	20–29 years	30–39 years	40–49 years	50–59 years	60–69 years
Passive data protection strategies									
Refrained from registering for online services (not wanting to provide personal information)	75	76	74	78	78	77	73	73	70
Stopped using certain websites (because of privacy concerns)	65	68	63	67	67	65	65	66	62
Refrained from registering for an online service (because of its data usage policy)	63	64	61	50	58	65	63	66	67
Refrained from buying certain products online (because of privacy concerns)	57	57	56	55	60	65	57	52	48
Active data protection strategies									
Updates anti-virus-software on a regular basis	95	97	92	89	96	95	94	95	97
Uses anti-malware-software to detect potential threats	85	90	79	85	83	86	86	86	81
Deletes cookies and cache regularly	84	88	79	76	82	89	85	84	80
Deletes browser history regularly	84	88	81	86	83	87	85	84	82
Used pseudonyms when registering for online services	53	58	48	70	72	68	46	40	29

(continued)

Table 1 (continued)

	Overall	Men	Women	14–19 years	20–29 years	30–39 years	40–49 years	50–59 years	60–69 years
Used unidentifiable e-mail address to register for online services	51	57	45	67	64	63	46	39	32
Used anonymization tools to obfuscate identity	35	43	27	40	50	45	33	25	18
Used encryption for e-mail communication	32	37	25	32	36	40	34	24	22
Used anti-tracking-software	32	39	24	35	40	41	31	24	21
Legal data protection strategies									
Asked online service providers not to share personal information with other companies	40	43	36	40	52	48	39	32	24
Asked online service providers to delete personal data	36	40	32	30	47	46	36	31	22
Basis: $N = 1932$									

they have read its data usage policy. The implementation of these rather facile strategies does not vary between men and women or young and older people.

With regard to active data protection strategies, the data present a rather mixed picture: whereas simple practices (from a technical point of view) such as updating and using anti-malware-software or deleting browser information are implemented by most users, pseudonymization or anonymization strategies are only used by a few users. Only half of the sample has used a pseudonym when registering for online services (53 %) or has created unidentifiable e-mail-addresses (51 %). In contrast, rather difficult and technically demanding strategies such as using anonymization tools (e.g., TOR, JonDonym) or encryption tools (e.g., PGP) are only implemented by less than a third of the sample. With regard to these practices, differences within the population are visible: male and younger participants were more likely to apply these tools than female and older participants. Corrective measures which require a lot of engagement and expenditure of time are also less prominent within the sample: only less than 40 % have already taken legal steps to safeguard their personal data. For example, only 36 % have asked online service providers to delete their personal information.

These results show that users seem to be willing to adopt simple and easily applicable strategies, but do not use complicated tools which require advanced technical skills or consume a lot of time. This is in particular problematic for the protection of institutional privacy because once users are not able to implement certain active DIY data protection practices such as using anonymization tools or encryption, the only remaining solution for effective data protection on a personal level is opting-out or using passive data protection strategies for that matter. Based on this rationale, it seems logical to assume that promoting online privacy literacy might be a good idea. Online privacy literacy has been said to "support, encourage, and empower users to undertake informed control of their digital identities".[33] Promoting privacy literacy might hence serve as a stopgap between inconsistent privacy attitudes and behaviors.[34] First studies in this field support this assumption: For example, many users feel unable to implement these specific privacy protection tools. For instance, only 35 % of German internet users feel capable of encrypting their e-mail communication.[35] As mentioned above, awareness of data collection and data mining practices presents a precondition for the implementation of DIY data protection practices, yet many users are not aware or at least do not have insights into these practices. A representative study with

[33]Park, "Digital Literacy and Privacy Behavior Online," 217.

[34]Sabine Trepte et al., "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," in *Reforming European Data Protection Law*, ed. Serge Gutwirth, Ronald Leenes, and Paul de Hert (Dordrecht: Springer, 2015), 333–366.

[35]Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), "DIVSI Studie zur Freiheit versus Regulierung im Internet," (Hamburg, 2013), accessed March 10, 2015. https://www.divsi.de/wp-content/uploads/2013/12/divsi-studie-freiheit-v-regulierung-2013.pdf.

German internet users for example found that 33 % of the participants did not know that website providers combine information from different websites to create user profiles.[36]

Summing up, it can be said that a third of the German population does implement DIY privacy protection strategies, however, the data also show that effective and comprehensive data protection with regard to institutional privacy—which requires to implement also more sophisticated measures—seems to be very difficult to achieve for the most individual users. Being aware of and understanding the technical architecture behind online information flows becomes harder and more complex with the rapid growth of new technologies. Furthermore, data protection itself becomes more and more complex. Although many and singular strategies and tools—which can only help to protect certain aspects of online privacy—exist, a universal remedy in form of a single strategy is not available. Keeping up with new technologies, tools, and strategies, requires time, competence and resources. As such, data protection is at risk of becoming limited to those who can spare the effort to learn handling data protection technologies. Differences in privacy literacy may hence foster a divide between those who are able to ensure data protection and those who are not.

That being said, it is noteworthy to add that absolute data protection (with opting-out as final solution) is mostly not desirable for most users. In many contexts, the sharing of information is appropriate. Depending on contextual factors such as norms, actors, attributes and corresponding transmission principles, user might not feel that their privacy is violated and their contextual integrity is hence preserved.[37] Scholars have found that the use of the social web and other online services satisfies many other needs that have to be taken into account when assessing users' behavior regarding privacy. The following paragraph will hence discuss to what extent the need for privacy in online environments competes with other forms of need satisfaction.

2.2 Competing Needs: Privacy and Data Protection Versus Social Gratifications

To dissolve the seeming paradox between users' privacy concerns and their actual online behavior, many researchers have argued that people refrain from implementing data protection strategies because they benefit from advantages and

[36]Trepte et al., "How Skilled Are Internet Users When it Comes to Online Privacy and Data Protection? Development and Validation of the Online Privacy Literacy Scale (OPLIS).".

[37]Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford Law Books, 2010).

gratifications that online services have to offer.[38,39] Buying products via online-shops, booking trips via online services, or simply using online-banking is fast, easy, and convenient. Specifically through the use of social web platforms, users are able to obtain a number of gratifications. Self-disclosure can be defined as "the process of making the self known to others"[40] and as such is a basic requirement for social interactions and communications. Disclosing private information to other people fosters social proximity.[41] Sharing personal information in the social web can hence lower barriers of initial interaction, leads to social acceptance and relationship-building, and provides users with feedback regarding their own identity formation.[42] Accordingly, it has been argued that users weigh the risks and benefits of online self-disclosure.[43] It seems plausible that users voluntarily take the risks involved with self-disclosure in order to obtain desired gratifications. However, although these needs might indeed compete with each other at certain times, this balancing is not a zero-sum game: People are in particular open and willing to share personal information if they perceive a situation as private.[44] Creating a safe and secure platform, on which one is able to disclose personal information without fearing privacy violations might hence be more desirable for users than complete withdrawal from social interaction in online realms. The balancing of costs and benefits of use however rests on the assumptions that user always have the choice between using or not using a service. Yet, in many cases, individuals have to engage with certain services or are dependent on them to achieve certain goals (e.g., finding a job, getting or staying on contact with certain people…). In these cases, an individual cost-benefit analysis might be very limited.

Individual aims and concerns that structure the importance and motivation to engage in data protection practices have their equivalent among the advocates of DIY data protection; and yet, the latter's arguments are very much entangled in social and political contexts. Consequently, such contexts are of central relevance

[38]Monika Taddicken and Cornelia Jers, "The Uses of Privacy Online: Trading a Loss of Privacy for Social Web Gratifications," in *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, ed. Sabine Trepte and Leonard Reinecke (Berlin: Springer, 2011), 143–156.

[39]Trepte et al., "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," 338.

[40]Sidney M. Jourard and Paul Lasakow, "Some Factors in Self-Disclosure," *Journal of Abnormal Psychology* 56, no. 1 (1958).

[41]Irwin Altman and Dalmas Taylor, *Social penetration: The development of interpersonal relationships* (New York: Holt, Rinehart and Winston: 1976).

[42]Nicole B. Ellison et al., "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment," in *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, ed. Sabine Trepte and Leonard Reinecke (Berlin: Springer, 2011), 19–32.

[43]Trepte et al., "Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," 338.

[44]Sabine Trepte and Leonard Reinecke, "The Social Web as a Shelter for Privacy and Authentic Living," in *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, ed. Sabine Trepte and Leonard Reinecke (Berlin: Springer, 2011), 143–156.

when it comes to analyzing the rather moderate success of promoting DIY data protection to date. Next, we will support this claim by presenting a cursory analysis of the German DIY data protection discourse as it is reproduced by some of the most influential participants.

2.3 DIY Data Protection Advocates and Their Socio-Political Entanglements

One way of conceiving DIY data protection—and a rather fruitful one, for that matter—is to view them as a specific form of *sociocultural* practice.[45] Practice, in this context, means that performing DIY data protection is a routinized everyday activity which does not consume much of the social actors' conscious awareness "but goes without saying"; the implicit nature of the knowledge that is involved points to the tacit character of such practical skills.[46] DIY data protection practices, that is, occur as embodied skills collectively developed, performed and maintained by "social worlds."[47]

The collective nature of the practices in question became visible already in the "early days" of DIY data protection. The so-called Cypherpunks, cryptography experts holding libertarian, and thus strong individualistic worldviews, belong to the most profound, and also most enthusiastic proponents of DIY data protection. In "A Cypherpunk's Manifesto", for example, Eric Hughes, one of the most prominent DIY data protection advocates, raised hopes in the early 1990s that "Cryptography will ineluctably spread over the whole globe, and with it the anonymous transaction systems that it makes possible."[48] Whereas such transaction systems, Hughes believed, are a necessary pre-condition for privacy to prevail, privacy itself would be a necessary pre-condition for an "open society".

Whatever one might think of such ideas, there is no doubt that cryptography did *not* spread around the globe; in other words, harnessing cryptography for DIY data protection was not translated into a mass phenomenon,[49] as Hughes stated in

[45]Paul Dourish and Ken Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *HUMAN-COMPUTER INTERACTION* 21 (2006): 319–342.

[46]In the sense of: Anthony Giddens, *The Constitution of Society: Outline of the Theory of Structuration* (Cambridge: Polity Press, 1984).

[47]Anselm Strauss, "A Social World Perspective," *Symbolic Interaction* 1 (1978): 119–128.

[48]Eric Hughes, "A Cypherpunk's Manifesto", accessed February 23, 2015. http://activism.net/cypherpunk/manifesto.html.

[49]More precisely speaking, cryptography did not spread globally as an everyday practice of average users for the sake of individual privacy protection, though it was, and is, in fact, harnessed by large corporations (business, public authorities) on a global scale to serve IT security ends.

2012—most people do not encrypt, say, emails, as a matter of course[50] (see also Sect. 2.1). Having said this, there is an obvious, yet overlooked reason for the absence of DIY data protection practices: the emergence of such practices presupposes the creation of a social (norms, codes of conduct), cultural (knowledge, skills, frames of meaning), legal (legal rules and regulations), technological (suitable soft- and hardware)—and so on—infrastructure that is to be generated by some collective body. In other words, creating DIY data protection practices is a collective endeavor, no matter how deeply engrained the individualism of DIY data protection proponents may be.

As a result, the creation of DIY data protection practices inevitably is a social process, which is why the dispute concerning cryptography that occurred in the early 1990s did not come as a surprise at all. In this sense, then, the emergence of DIY data protection practices in contemporary societies, whether based on cryptography or else, is likewise contested. For example, even a cursory look at the German discourse on DIY data protection demonstrates that the practices in question, if anything, may emerge in an environment that is a rather hostile one, due to the specific constellation of interests and resources of the actors involved. There are at least four groups participating in the discourse: technology activists, institutionalized data protectionists, political parties building the parliament, and trade associations. Interestingly, the grand majority of these groups, while pursuing rather dissimilar interests, equally call upon *the individual* to build practices of DIY data protection.[51]

For example, *activists* tend to portray public authorities as well as economic enterprises as being motivated to install surveillance techniques—either due to some intrinsic interest in controlling populations, or in maximizing data-driven profits respectively. Thus, it depends on individual citizens to protect themselves against such interests.

Data protectionists call upon individuals as civil right holders. Their perspective is normatively framed by the German right to informational self-determination, which states that, from a legal-normative view, in democratic societies individuals are entitled to know who knows what about them whenever and in any given context. Whereas the jurisdiction transcends the individual in that there are social dimensions taken into account and collective duties being inferred from the centering on the individual, the latter nevertheless builds the normative core of the legal reasoning. Consequently, data protectionists, insofar as they are bound to

[50]Ole Reißmann, "Cyptoparty-Bewegung: Verschlüsseln, verschleiern, verstecken," Spiegel-Online, October 9, 2012, accessed February 23, 2015, http://www.spiegel.de/netzwelt/netzpolitik/cryptoparty-bewegung-die-cypherpunks-sind-zurueck-a-859473.html.

[51]Obviously, I am talking about ideal types here that nevertheless coin the discourse on DIY data protection most profoundly.

official jurisprudence, tend to appeal to the individuals to exercise their rights thus trying to activate the individual to act.[52]

Political parties generally have a pretty ambivalent attitude towards data protection, and also towards individuals' performing DIY data protection practices. They necessarily strive to come into power in order to realize their political goals. However, once in power, they represent the state, and it is certainly fair to identify some intrinsic interest of the state in surveillance as regards the populations that public authorities are bound to manage, govern and supervise. Thus, Baumann, for example, when investigating political parties' positions on data protection in the last legislature, found a strong correlation between power and willingness to foster data protection: the more political power a politician is able to execute, the less s/he is interested in data protection.[53] Moreover, there is a perceived conflict of objectives when it comes to administration, insofar as it is the state's duty to safeguard citizens' safety and security, while at the same time being responsible to defend citizens' freedom. Verisimilitude (or lack thereof) of such trade-off argumentations aside, they serve as an instrument for public authorities to have their cake and eat it too: rhetorically they may applaud individuals for developing DIY data protection practices, while at the same time neglecting to take on responsibility for the collective emergence of such practices.[54]

Finally, *the information economy*, insofar as business models are based on harvesting social actors' digital traces, is all but interested in the emergence of DIY

[52]I will omit here that to a certain degree data protectionists are caught up in a specific double bind: while they are public authorities and thus subject to the state's agency, they at the same time are bound to protect citizens from illegitimate interventions effected by this very state.

[53]Max-Otto Baumann, "Datenschutz im Web 2.0: Der politische Diskurs über Privatsphäre in sozialen Netzwerken," in *Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter*, ed. Ulrike Ackermann (Frankfurt/M.: Humanities Online, 2013), 47.

[54]In this respect, the infamous statement of the former Minister of the Interior, Hans-Peter Friedrich, speaks volumes: On 16th of July 2013, Friedrich, at the time German Minister of the Interior, was interrogated by the parliamentary board that is supposed to supervise the intelligence service. Friedrich was asked about his state of knowledge concerning the so-called "NSA scandal". After having been interrogated by the board's members he faced the media. In this context Friedrich turned to German citizens, reminding them of their duties, asking them to assume their responsibilities, stating that they were supposed to learn by themselves how to cater for secure internet communication; in particular, Friedrich emphasized that cryptographic techniques and anti-virus software must be brought much more into focus. Also, the by-then Minister stated that people must become aware of the fact that also internet communications need to be protected. Thus we have here a perfect example for the shifting of the focus away from the extremely well-organized collective dimension of the civil rights attack carried out by the intelligence services to the individual's responsibility: DIY data protection serves as a way to individualize the social conflict, and to neglect the collective nature of the practices in question.

data protection practices in the sense of a mass phenomenon.[55] For the time being, it is not very hard for the spokespersons of the information economy—at least as far as the German discourse is concerned—to rhetorically foster the strengthening of the individuals' skills regarding data protection while at the same time giving them a run for their money if it comes to properly navigate privacy settings and so on. Quite obviously, the spread of DIY data protection practices would preclude a manifold of business models being based on harvesting personal information. Thus, businesses following such a model by definition cannot be interested in practices that threaten harvests. At the same time, however, it is very convenient to call upon individual consumers to develop such practices, while knowing that the emergence of these practices is no individual affair at all.

Thus, to summarize, while activists and data protectionists may have an interest in the wide-spread creation of DIY data protection practices, they have no resources to nourish the soci(o-technic)al processes that are required to effectively foster the development of those practices; conversely, the latter two groups do have access to resources,[56] but "by nature" they have no interest in citizens being versed in DIY data protection. For the reasons identified the odds are stacked against the wide-spread emergence of DIY data protection practices. However, as long as the most influential actors do not take on their responsibility in developing the collective, heterogeneous infrastructure that is the *sine qua non* for DIY data protection practices to evolve, the propagation of such practices may have undesired political repercussions, since it allows responsible entities to shift the burden to all those selves who are called upon to do data protection themselves. The normative implications of these shifts will be discussed in the following sections.

[55]This is not to say that, say, email service providers did not make use of encryption at all; German webmail service gmx, for example, provides encryption between end user and the company's mail servers, as well as among all the servers belonging to the so-called "E-Mail made in Germany"-network (an association of several Germany based email service providers, such as T-Online and WEB.DE). However, this may be interpreted as a rather superficial strategy to put the minds of worried users at rest, and not at all as the implementation of strong DIY data protection practices. More generally speaking, what I am referring to is the fact that in contemporary socio-technical assemblages it is players belonging to the surveillance *economy* that provide for the infrastructures enabling people to build up sociality. In modern societies, at least as far as European ones are concerned, *the state* used to be the agency that provided populations with the means to construct social structures (telegraph, mail, cable networks, you name it) and it also used to be *the state* that in turn observed the sociality thus built; in recent years, private corporations have become the main providers of key infrastructures of sociality (Online Social Networks serve as a paradigmatic case in point), as well as the main observers of the latter. As return on investment for most of these corporations is fundamentally, totally, absolutely grounded on the observation of the sociality built by "users" (who uses whom here?), the wide-spread emergence of strong DIY data protection practices is not in their interest as a matter of principle.

[56]For example, they could issue laws, install regulating bodies, strengthen relevant education (the state), or develop privacy friendly systems, make their techno-economic structure transparent, and effectively follow suitable business ethics.

3 DIY-Data Protection—Should We Have to Do It?

To answer this question we need to take a step back. In many regulatory frameworks data protection means to prohibit uses of data that would limit the citizens' ability to determine themselves who can access or use personal data and for what purposes. Our paper focuses rather on technological approaches than regulatory frameworks. In a sense, those technologies emphasize personal autonomy even more, since they need not rely on the legal and regulatory instruments; their development and use is often pursued by communities which are quite suspicious of the state (such as, e.g., the "cypherpunk movement", see Sect. 2.3).[57]

Yet, data protection has to be seen in a wider scope. Rather than asking how individuals can protect their data, the question should be: If citizens need data protection in the sense that particular pieces of data should not be accessible to particular actors, who should be responsible for that? This entails that an answer to this question also could change what data protection means or aims at.

This wider scope has several advantages: First of all, we need it to find alternatives for those cases where individual data protection simply is not feasible as Sect. 2.1 shows. But even if—for the sake of argument—these pragmatic concerns could be overcome, the wider scope still would be important.

This is because individual data protection needs a partition of responsibility: who is able to decide about which data? Terms such as "personal data" or "personal identifying information" are used in attempts to give citizens enough control over "their" data without their decisions infringing on others. In times of "Big Data", however, such a partition of responsibility becomes increasingly difficult. Louise Amoore has convincingly shown that not so much personal data but "data derivatives" are at the center of data based surveillance.[58] That is the relations and aggregates of data are more important than individual data sets. These kinds of technologies and data analyses are not only a challenge for individual concepts of privacy and data protection. They even disrupt the partition of privacy norms into wider social contexts as has been famously proposed by Nissenbaum[59]: The problem is that even if a citizen could fully transparently and conscious of the consequences for her or him decide in accordance with the contextual privacy norms, this data can still be used to infringe the privacy of *others*.[60]

---

[57]This, however, does not mean that the use of data protection tools cannot conflict with legal provisions. This can be seen in repeated calls to regulate the use of encryption as well as the legal constraints of the right to privacy, e.g. for the purpose of criminal investigations.

[58]Louise Amoore, "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times," *Theory, Culture & Society* 28 (2011).

[59]Nissenbaum, "Privacy in Context: Technology, Policy, and the Integrity of Social Life".

[60]Tobias Matzner, "Why Privacy is not Enough Privacy in the Context of 'Ubiquitous Computing' and 'Big Data,'" *Journal of Information, Communication & Ethics in Society* 12 (2014).

As a first step then, a wider, social perspective is necessary in the following sense: Even if the citizens would be responsible for data protection, it must be seen as a *social responsibility* and not as an individual problem. Everyone has to protect data they provide and use—even if it appears to be data "about them" and they think they have "nothing to hide"—because the data can be used to invade the privacy of others. As the results from the study presented in Sect. 2.1 shows, such concerns do not play a role or are even unknown to users. They mostly engage in data protection strategies which serve to protect their social privacy thus concentrating on protecting singular information against misuse.

As this reasoning illustrates, the question: "If citizens need data protection, who should be responsible for that?" opens up many more alternatives than just shifting, as it were, the workload of data protection. It also clarifies that responsibility by the citizens might either mean: "everyone is responsible for their own data protection", or "we are collectively responsible for our data protection." Many of the DIY data protection tools discussed here can be used to support either aim, but are usually advocated just concerning the first perspective.

It is important to note that this turn away from individual self-determination concerning data does not necessarily entail to give up other means of self-determination. To the contrary, it can even support them: Sect. 2.2 shows that data protection often competes with other needs or aims of self-disclosure. Dispensing with data protection or even voluntarily providing data can lead to increased social contacts, better carrier opportunities and many more. Yet, these arguments run the risk of remaining caught within the same logic of subsuming data protection (respectively forgoing it) under the aim of creating individual self-determination. The fact that problems or impediments in protecting data (currently) coincide with the aims of identity management of some or many individuals does not solve the underlying question of responsibility. Accordingly, we need to see the question who should be responsible for data protection in the wider context of distributing responsibilities among individuals, the state, and corporations—and thus also in the context of what individuality or at least individual freedom entail. This problem will be discussed in the next section under the rubric of "responsibilization". Before discussing this concept, however, it is important to remark that this argument concerns widespread data protection for the citizens. DIY-data protection tools are very valuable for particular persons or social actors like whistleblowers, journalists, or NGOs and other activists. Often their activities are important factors for changes on the wider political level that we discuss in the following section. And these activities include or even rely on DIY-data protection technologies—but also on using them in a very experienced and thoughtful manner. Thus, these technologies can be an important tactical tool for political activity as well as an indispensable protection for those who have no other choice.

3.1 Responsibilization

The term "responsibilization" has been coined in governance and criminology discourses and refers to "to the process whereby subjects are rendered individually responsible for a task which previously would have been the duty of another—usually a state agency—or would not have been recognized as a responsibility at all."[61] Usually it is discussed as a neo-liberal mode of governance that has been developed with recourse to Foucault's reflections on governmentality.[62] For example it can be seen in the transformation of the welfare state where citizens increasingly have to make their own provisions for former governmental benefits like health insurance or pension funds.

This perspective of governance is important concerning data protection, when public officials or institutions provide incentives and programs to propagate DIY data protection—as has been described in Sect. 2.3. Yet, we first want to focus on the underlying logic concerning individual actions in a broader sense. Lemke describes this as achieving congruence "between a responsible and moral individual and an economic-rational actor." To be responsible and moral is equated with rational self-determined choices: "As the choice of options for action is, or so the neo-liberal notion of rationality would have it, the expression of free will on the basis of a self-determined decision, the consequences of the action are borne by the subject alone, who is also solely responsible for them."[63]

Bennett and Raab describe the prevailing "privacy paradigm" as based on liberal theory, which "rests on a conception of society as comprising relatively autonomous individuals".[64] The authors show that this yields a particular concept of privacy, which has been criticized from several perspectives and is not without alternatives.[65] Still, though, it is this very concept of privacy that forms the background for most DIY data protection practices. Within the perspective of responsibilization, the named privacy paradigm is, as it were, relegated to a particular space of action for particular individuals that co-depend on social and technical conditions. Importantly, this foucauldian view does not simply say that the liberal privacy paradigm is wrong, but clarifies how it emerges from a particular configuration of states and private actors. Couched in slightly different, albeit cognate terms, such a view makes visible that the privacy paradigm described by Bennett and Raab is the product of a particular socio-technical configuration. A configuration, however, to

[61]Pat O' Mailey, "Responsibilization," in *The SAGE Dictionary of Policing*, ed. Alison Wakefield and Jenny Fleming (London: SAGE, 2009), 276.

[62]David Garland, "'Governmentality' and the Problem of Crime: Foucault, Criminology, Sociology," *Theoretical Criminology* 1 (1997).

[63]Thomas Lemke, "'The birth of bio-politics': Michel Foucault's lecture at the Collège de France on neo-liberal governmentality," *Economy and Society* 30 (2001): 201.

[64]Colin J. Bennett and Charles D. Raab, *The Governance of Privacy* (Cambridge: MIT Press, 2006), 4.

[65]Bennett and Raab, *The governance of privacy*, 14.

which it contributes in an essential way: By treating this confined space of action and individuality within the liberal perspective, the conditions producing it are neglected. Thus, the consequences of their actions are conceived as solely the individuals' responsibility.

This logic of responsibilization has several implications for data protection, which will be discussed in the following sections of this paper:

- Not engaging in data protection activities is seen as choice—equal to doing so (Sect. 3.2).
- Data protection becomes a commodity and the protected individuals become consumers (Sect. 3.3).
- Social inequalities concerning data protection cannot be addressed sufficiently, which may lead to victim blaming (Sect. 3.4).

While these points show the problems of locating data protection primarily with the individual, these results must be contextualized within the inherent ties between the logic of responsibilization and surveillance. Thus, paradoxically, individual data protection might seem the only remedy against the implications of responsibilization, if this logic is not addressed on a social-political level. This will be discussed in Sect. 3.5.

3.2 Data Protection as Choice

Positing the possibility for individual choice and data protection as created by socio-technical conditions does not necessarily devaluate self-determination as an aim for policy. It has, however, to be conceived of as the *creation* of possibilities and subject positions. If it is merely seen in the liberal perspective as the shielding from external interferences, it can very well be that even in the absence of any interference the desired action remains impossible. This is the case concerning data protection: Sect. 2.1 shows the purely pragmatic problems of DIY data protection. It is increasingly difficult to grasp the consequences of a person's decisions concerning their data. This is a precondition for responsible actions from the liberal perspective that is as of now almost impossible to attain. The tools which are available are hard to use properly and involve competence and resources. If these structural problems are ignored, the danger arises that data protection regulations shield a space for autonomous decisions that, however, are impossible to carry out. Thus, basic rights to privacy are hollowed out. As a first result, this shows: If the citizens have to protect their privacy on their own, they can only do it based on active provisions by the state and commercial actors—as has already been emphasized at the end of Sect. 2.3—or at least with a considerable extent of self-organization and citizen-led structures.

The logic of responsibilization brings about further ramifications: All kinds of behavior concerning data, and in particular, not engaging in data protection activities, are considered as (rational) choice. This is maybe most salient in refusals to introduce better privacy policies by corporate actors. Often they argue that people who are not content with the level of data protection should just not use their services or products. This presupposes that using or not using a particular service are equal choices. Such an assessment of course depends on the product in question. But generally we can say that this presupposition is often not met on several levels:

The first concerns transparency and coercion: The reasons for not using a service or product are usually buried deeply in license agreements or privacy policies we have to "consent" to before using.[66] The reasons to use them, on the contrary, are promoted by the best advertising agencies in the world. Furthermore, big IT companies are actively advocating the use of their products in education and the workplace,[67] thus spreading a lax data protection regime, which may be compulsory in school or at the workplace. Often such conditions can only be evaded at the high social cost of changing the school or the employer or by organizing resistance and asking for different infrastructure from a dependent position. This leads on to the next problem of framing not to use a service or product as alternative choice. Information and communication technology has pervaded almost every aspect of our lives. In particular smartphones are almost considered as a standard in many contexts in Europe and the USA.[68] Although they are still a commodity that theoretically everyone chooses freely to buy and use, in effect most people who decide to refrain from using them might face more or less severe social costs: less contacts with friends, missing carrier opportunities, more complicated dating, being considered inefficient as a colleague, being considered suspicious at border controls, and many more. Of course, these examples are hardly comparable concerning severity and consequences. But the motley list shows both the variety of aspects of life that are permeated by this technology and the respective breadth of problems that refusing to use a smartphone can cause. In fact, vendors openly advertise the very benefits one will be missing without a smartphone. This reproduces a structure quite common within the logic of responsibilization: an individual/socio-technical asymmetry where the possibilities of the socio-technical changes provided by corporate actors are openly endorsed, whereas the problematic consequences and responsibility lie with the individual alone.

---

[66]On the problematic pragmatics of license agreements, see for example Debatin et al.: "Facebook and online privacy for social networking sites," or Chee et al., "Re-Mediating Research Ethics" concerning games.

[67]See for example Apple's "iPad in Education" website: https://www.apple.com/education/ipad/ (accessed February 19, 2015).

[68]In Europe, more than half of all persons already own a smartphone, with a continually growing market predicted: http://www.statista.com/statistics/203722/smartphone-penetration-per-capita-in-western-europe-since-2000/ (accessed March 4, 2015).

This is by no means a matter of course for widely used commodities. To the contrary, recognizing the importance of ICT for our daily lives can warrant high levels of regulation, like those already in place for many other important goods—their being a commodity on a free market notwithstanding: e.g. food, drugs, or cars.

3.3 Data Protection as Commodity

We have already touched upon many points that could also fall under this rubric in the last section. Here, however, we want to focus less on the implications of certain commodities like smartphones concerning data protection. We rather want to discuss data protection itself becoming a product or at least a price relevant product feature and thus something that is attainable for money. In the context of the infeasibility of completely individual data protection, users of ICT have to entrust some other actor or institution with data protection tasks. The need to build a trustworthy environment has long been considered as an important factor in the IT business[69] but in particular after the revelations by Edward Snowden, data protection has increasingly become a feature for selling products—and the market for data protections as a product by itself is growing. Such products come in many variants: encryption software for many channels of communication (mail, chats, voice), hardware products like encrypted phones or personal servers to run one's own "cloud", subscription services for encrypted and anonymized communications, and many more. Other providers sell privacy as a kind of "add-on" like AT&T's offer not to track their internet subscribers' activities for an additional 29 US dollars.[70]

Of course such products are premised on the condition that the providers are trustworthy in the first place—which is dubitable concerning the revealed powers of secret services to avail themselves of commercially collected and administrated data. Yet, as we note in Sect. 2.1, data protection has many opponents, not only secret services. And concerning many of them, in particular social privacy, commercial data protection products might be a sensible solution. In the end, providers who want to prevail on a market should not be too abusive of the trust of their customers.

This solution, however, replaces the requirements of competences and time, which render DIY data protection impractical, with another requirement: money.[71] Given the omnipresence of IT, this would entail that almost everyone would have to spend some extra money to get data protection. This need arises in a context

[69]Bennett and Raab, The Governance of Privacy, 53 et seqq.

[70]http://arstechnica.com/business/2015/02/att-charges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing/ (accessed February 19, 2015).

[71]Of course, providing competence and time is usually more or less directly related to monetary costs as well.

that is by no means a level playing field for two reasons: money is unequally distributed and data protection needs are unequally distributed. While the first is a matter of course, the second aspect deserves some words: Maybe most problematically, researchers like John Gilliom have shown that many surveillance activities (and thus an increased need for privacy protection) focus on those that do not have much money. Here the responsibilization of data protection becomes entangled with other responsibilization processes concerning welfare. Very often such processes of responsibilization require increased data collection and legitimize surveillance.[72] That does not only mean that those with the least money would have the biggest need to spend—in itself problematic enough—but that such products are ineffective for them since they are under surveillance through other channels.[73]

Many other groups that face the threat of social stigma or discrimination have higher data protection needs as well: e.g. women, homosexuals, migrants, or members of certain religions. Data protection as a commodity thus entails higher financial burdens for those social identities. Thus, we run the risk of privacy becoming a luxury for those who can afford it. And furthermore, this additional cost is especially put on those who already face discrimination or social inequalities.

Considering the argument in Sect. 3 that data protection can only be achieved socially, however, this luxury will not have much worth. If not enough people buy in, there will be sufficient data available to create the data derivatives that are of interest anyway. This shows that customer choice is just a very explicit instance of the logic of individual choice discussed in the last section—and thus reproduces the problems discussed there.

3.4 Data Protection, Social Equality, and Victim Blaming

To discuss this aspect, first of all we have to emphasize that users of social media and other ICTs do care for their privacy—even if they disclose all kinds of information.[74] Some, in particular teenagers and children even perceive online interaction as more private since it is more easily shielded from parents or teachers—their preeminent threat to privacy.[75] Thus, online interaction is structured by complex privacy needs and requirements even where people voluntarily

[72]John Gilliom, *Overseers of the Poor* (Chicaco: Chicago University Press, 2001), 130 et seqq.; Nikolas Rose, "Government and Control," *British Journal of Criminology* 40 (2000).

[73]More on this in Sect. 3.5.

[74]See also Sect. 2.

[75]Valerie Steeves, "Data Protection Versus Privacy: Lessons from Facebook's Beacon," in *The contours of privacy*, ed. David Matheson (Newcastle: Cambridge Scholars Publishing, 2009), 187.

provide substantial amounts of data.[76] Steeves argues that a focus on data protection cannot grasp this complexity since it is limited to data and the procedures of its usage, while the actions which yield that data are structured by a wider normative social context.[77] In particular, this focus on the data within the logic of responsibilization means that the data is conceived as provided by choice. As Sect. 2.2 shows, privacy considerations stand in a complex context of other aims and motives but also requirements and coercions. Within the logic of responsiblization, this context only figures insofar as the provision of withholding of data is taken to be the rational choice balancing the various aims and requirements—and if that rational choice did not take place, this is the individual's shortfall.

From an individual point of view, however, interaction is not structured by access and use of data but by the entire complex bundle of norms of action. These norms very well might coerce individuals into disclosing private information or lead to the endorsement of actions that entail providing private data. That does not mean that these persons endorse all the kinds of uses of their data that could be justified by their individual refusal (viz. choice) to keep that data completely private.

Importantly, such privacy norms are not equally distributed. For example, Bailey et al. have researched young women's perception of Facebook profiles. The teenage participants of the study clearly perceived Facebook as a "commoditized environment" where "stereotypical kinds of self-exposure by girls are markers of social success and popularity."[78] For young women, these stereotypes involve providing more private information compared to men: details about their relationships (often including the partner on the profile picture), details about their friends and more intimate pictures, e.g. shots in bikinis. While many of the participants have been critical about such profiles, most have clearly admitted the social success that can be achieved by following these norms. That shows that women face a broader requirement of choices concerning privacy that do not arise for men. If the individuals are held responsible for their use and protection of their data, this means increased burdens for women. Furthermore, when deciding for data protection (which in this case means not providing the data) their socials costs are higher.

Individual responsibility for data protection clearly leads to unequal distribution of effort, material and social costs that materialize along social lines of discrimination—in this example gender. These differences disappear from view when the focus is put on data protection and individual responsibility that mainly asks who did or did not provide which kinds of data. Thus, the responsibility problems or misuse arising from the private or intimate data is attributed to the women, since they did provide the data in the first place, when they could have "simply"

[76]This, of course is the rationale of Nissenbaum's approach in "Privacy as Contextual Integrity" that she has developed from reflections on "privacy in public."

[77]Steeves, "Data protection vs. Privacy," 189.

[78]Jane Bailey et al., "Negotiating With Gender Stereotypes on Social Networking Sites: From 'Bicycle Face' to Facebook," *Journal of Communication Inquiry* 37 (2013): 91.

not done so. It is this last supposition that evades the social circumstances and leads to victim blaming.

The logic of individual responsibility concerning data protection thus can contribute to the proliferation of such moral double standards since it is hard to address the "moral climate" in which needs and social costs of data protection arise, when the focus lies only on the individual and the question whether data is accessible or not.

This also precludes emancipatory movements for the freedom to be as explicit and open as one wishes. The act to publish the data despite the moral double standards to appropriate the practice (in this case posting pictures or having private data on facebook) must explicitly posit oneself against the existing norms to not fall prey to the logic of commodification, control and blame.[79]

3.5 Responsibilization, Surveillance, and Politics

The outsourcing of responsibilities and services from the state or corporate actors towards the individual here discussed as "responsbilization" brings about needs for monitoring and surveillance. For example, a common practice in health insurance is to provide incentives for regular medical checks or "healthy" activities like sports or exercises. For this to work, however, the behavior of the clients has to be monitored beyond that which happens in physicians' practices, for example including leisure activities or diets. Of course, when increasingly responsibility is moved to the citizens, also the state's monitoring increases. In fact, the process of responsibilization is closely tied in with surveillance and control.[80] Security then is established within a preemptive logic that tries to sort individuals based on intensive monitoring.[81] Responsible and moral citizens of course will not get into the focus of these practices—only suspect persons will—as security agencies all over the world emphasize. But everybody, again, is responsible for being that particular kind of responsible and moral citizen—also regarding the data they provide and use.

Thus, many of the reasons for an increased need for data protection arise within the logic of responsibilization itself—adding data protection as one further field to look after. Here, however, the logic turns against itself, when the citizens try to inhibit surveillance and thus an intrinsic part of responsibilizationist control. Still, the logic remains intact when states try to support the development and marketing

[79]See for example the problems of legislating revenge porn without reproducing the logic of victim blaming or infringing the sexual liberty of women in Henry and Powell, "Beyond the 'sext'".

[80]Rose, "Government and control."

[81]David Lyon, "Surveillance As Social Sorting," in *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*, ed. David Lyon (New York: Routledge, 2003).

of privacy enhancing technologies for the end-consumer market. But states try to establish conditions where DIY data protection can be carried out as a flourishing market but under conditions where these practices do not inhibit state surveillance.[82] The revelations of secret services spying on citizens attest to that. So it is only natural from that point of view that the requirement of government backdoors was immediately voiced when stronger encryption paradigms have recently been rolled out in mobile communications.[83]

In such a climate it may seem rather naïve to entrust anyone but oneself with data protection. Furthermore, since resisting surveillance turns against the logics of responsibilization as just described, it might appear as a valid move of resistance. To an extent, this is true. But it would be mistaking the cause for the symptoms. Much of the states' surveillance is not done by eavesdropping on individuals but by helping themselves to the big databases that accrue in other places like big online enterprises. In a society where most services are commodities and keeping track on customers is part of a business model focused on ever increasing efficiency marketed as individualization, the data which is of interest for commercial actors and security agencies often coincide.[84] In a society where welfare and insurance is detached from communitarian models and broke up into individual provisions again based on circumspect data collection, even more data of interest for secret services is generated. Thus, many of the possibilities to collect data in the first place rise from the commodified and responsibilized societies we life in. Then DIY data protection is an almost vain attempt to fight a functional process of these societies while ignoring the rest—or even keeping it intact and alive by adding data protection as another flourishing branch on the market.

4 Conclusion

A move towards data protection that takes such reflections into account must address the many causes of the accrual of data on a political and social level rather than taking them for granted and trying to evade them where possible. This would entail to call on the state to take its responsibilities in protecting its citizens' data seriously, and not only to enable markets. It also needs to address national security as universal subterfuge from European data protection legislation.

On a more fundamental level, the implications of data protection as a social responsibility have to be assessed. Initiatives to foster data literacy or media literacy can still be a valuable tool, when they include social perspectives and in particular address the unequal distribution of data protection needs in society.

[82] See the quote above in note 50 as an example.

[83] http://www.slate.com/blogs/future_tense/2015/01/19/obama_wants_backdoors_in_encrypted_messaging_to_allow_government_spying.html (accessed March 4, 2015).

[84] Jeffrey Rosen, *The naked crowd: Reclaiming security and freedom in an anxious age* (New York: Random House, 2005), Chap. 3.

The imbalance of choosing to use a service versus not using it can be mediated by sensible data protection defaults that emphasize data protection and need an active decision to enable less protective uses. Of course the problems of making that choice in a transparent and reflected manner remain. Albeit, it is better to actively demand accepting that data may be used in ways that are almost impossible to know rather than making it the default. And such defaults mainly address the collection of data but not the processing, sharing, and analysis.

On an institutional level, intermediaries between the citizens on the one side and the state of corporations on the other can organize data protection. Consumer protection models are one possibility. Another way is *social* self-organizing. Many communities in fact have conscious discussions or rules concerning privacy among their members, which include but are not restricted to data protection policies. Often, these are groups that are faced with higher privacy requirements, e.g. online self-help communities. Albeit, practices that are developed by such groups still can be a model for others.

Empirically speaking, the wide-spread emergence of DIY data protection practices is rather improbable, or more precise: As long as (also DIY!) data protection is not considered a collective, profoundly political endeavor, DIY data protection is an ill-fated practice. What's more, without taking on a collective perspective, the advocating of DIY data protection may even create undesired effects, for it allows for neglecting political responsibility, fostering further inequalities between users, and generally asking too much of the individual.

Bibliography

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42: 249–274.

Altman, Irwin, and Dalmas Taylor. 1976. *Social penetration: The development of interpersonal relationships*. New York: Holt, Rinehart and Winston.

Amoore, Louise. 2011. Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28: 24–43.

Bailey, Jane, Valerie Steeves, Jacquelyn Burkell, and Priscilla Regan. 2013. Negotiating with gender stereotypes on social networking sites: From "bicycle face" to facebook. *Journal of Communication Inquiry* 37: 91–112.

Barnes, Susan B. 2006. A privacy paradox: Social networking in the Unites States. *First Monday* 11(9). doi:10.5210/fm.v11i9.1394. Accessed 10 Mar 2015.

Baumann, Max-Otto. 2013. Datenschutz im Web 2.0: Der politische Diskurs über Privatsphäre in sozialen Netzwerken. In *Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter*, ed. Ulrike Ackermann, 15–52. Frankfurt/M.: Humanities Online.

Bennett, Colin J., and Charles D. Raab. 2006. *The governance of privacy*. Cambridge: MIT Press.

Brandtzæg, Petter Bae, Marika Lüders, and Jan Håvard Skjetne. 2010. Too many Facebook 'friends'? Content sharing and sociability versus the need for privacy in social network sites. *Intl. Journal of Human-Computer Interaction* 26: 1006–1030.

Chee, Florence M., T.Taylor Nicholas, and Suzanne de Castell. 2012. Re-mediating research ethics: End-user license agreements in online games. *Bulletin of Science Technology & Society* 32: 497–506.

Debatin, Bernhard, Jenette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer Mediated Communication* 15: 83–108.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI). 2013. DIVSI Studie zur Freiheit versus Regulierung im Internet. Hamburg. https://www.divsi.de/wp-content/uploads/2013/12/divsi-studie-freiheit-v-regulierung-2013.pdf. Accessed 10 Mar 2015.

De Wolf, Ralf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35: 444–454.

Dienlin, Tobias, and Sabine Trepte. 2014. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*.

Dourish, Paul, and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction* 21: 319–342.

Ellison, Nicole B, Jessica Vitak, Charles Steinfield, Rebecca Grey, and Cliff Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy online. Perspectives on privacy and self-disclosure in the social web*, ed. Sabine Trepte, and Leonard Reinecke, 19–32. Berlin: Springer.

Garland, David. 1997. 'Governmentality' and the problem of crime: Foucault, criminology, sociology. *Theoretical Criminology* 1: 173–214.

Giddens, Anthony. 1984. *The constitution of society: Outline of the theory of structuration*. Cambridge: Polity Press.

Gilliom, John. 2001. *Overseers of the poor*. Chicaco: Chicago University Press.

Gunkel, David J. 2003. Second thoughts: Towards a critique of the digital divide. *New Media & Society* 5: 499–522.

Henry, Nicola, and Anastasia Powell. 2014. Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*. doi:10.1177/0004865814524218. Accessed 10 Mar 2015.

Hughes, Eric. 2015. A Cypherpunk's Manifesto. http://activism.net/cypherpunk/manifesto.html. Accessed 23 Feb 2015.

Jourard, Sidney M, and Paul Lasakow. Some factors in self-disclosure. some factors in self-disclosure. *Journal of Abnormal Psychology* 56(1): 91.

Lampinen, Airi, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: Interpersonal management of disclosure in social network services. *Proceedings of the SIGCHI conference on human factors in computing systems*, 3217–3226. New York, USA: ACM.

Lemke, Thomas. 2001. 'The birth of bio-politics': Michel Foucault's lecture at the Collège de France on neo-liberal governmentality. *Economy and Society* 30: 190–207.

Litt, Eden. 2013. Understanding social network site users' privacy tool use. *Computers in Human Behavior* 29(4): 1649–1656.

Lyon, David. 2003. Surveillance as social sorting. In *Surveillance as social sorting: Privacy, risk, and digital discrimination*, ed. David Lyon, 13–30. New York: Routledge.

Masur, Philipp K, and Michael Scharkow. Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. (in prepartion).

Masur, Philipp K., Doris Teutsch and Sabine Trepte. *Entwicklung der Online-Privatheitskompetenz-Skala*. (in preparation).

Matzner, Tobias. 2014. Why privacy is not enough privacy in the context of 'ubiquitous computing' and 'big data.' *Journal of Information, Communication & Ethics in Society* 12(2):93.

Milne, George R., and Andrew J. Rohm. 2000. Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing* 19(2): 238–249.

Metzger, Miriam J. 2007. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication* 12: 351–361.

National Telecommunications and Information Administration (NTIA). 2015. Falling through the net: A survey of the 'have-nots' in Rural and Urban America. Washington, DC: US Department of Commerce. http://www.ntia.doc.gov/ntiahome/fallingthru.html. Accessed 10 Mar 2015.

Nissenbaum, Helen. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford: Stanford Law Books.

O' Mailey, Pat. 2009. Responsibilization. In *The SAGE dictionary of policing*, ed. Alison Wakefield and Jenny Fleming, 276–278. London: SAGE.

Papacharissi, Zizi A. 2010. *A private sphere: Democracy in a digital age*. Cambridge: Polity Press.

Park, Yong J., Scott W. Campbell, and Nojin Kwak. 2012. Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior* 28(3): 1019–1027.

Raynes-Goldie, Katie. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday* 15(1). http://firstmonday.org/article/view/2775/2432. Accessed 10 Mar 2015.

Reißmann, Ole. 2012 Cyptoparty-Bewegung: Verschlüsseln, verschleiern, verstecken. *Spiegel-Online*. http://www.spiegel.de/netzwelt/netzpolitik/cryptoparty-bewegung-die-cypherpunks-sind-zurueck-a-859473.html. Accessed 23 Feb 2015.

Rogers, Everett M. 2005. *Diffusion on innovations*. New York: Free Press.

Rose, Nikolas. 2000. Government and control. *British Journal of Criminology* 40: 321–339.

Rosen, Jeffrey. 2005. *The naked crowd: Reclaiming security and freedom in an anxious age*. New York: Random House.

Selwyn, Neil. 2004. Reconsidering political and popular understandings of the digital divide. *New Media & Society* 6: 341–362.

Skouma, Georgia, and Laura Léonard. 2015. On-line behavioral tracking: What may change after the legal reform on personal data protection. In *Reforming European Data Protection Law*, ed. Serge Gutwirth, Ronald Leenes, and Paul de Hert, 35–62. Dordrecht: Springer.

Steeves, Valerie. 2009. Data protection versus privacy: Lessons from Facebook's Beacon. In *The contours of privacy*, ed. David Matheson. Newcastle: Cambridge Scholars Publishing.

Strauss, Anselm. 1978. A social world perspective. *Symbolic Interaction* 1: 119–128.

Taddicken, Monika, and Cornelia Jers. 2011. The uses of privacy online: Trading a loss of privacy for social web gratifications. In *Privacy online. Perspectives on privacy and self-disclosure in the social web*, ed. Sabine Trepte, and Leonard Reinecke, 143–156. Berlin: Springer.

Trepte, Sabine, Tobias Dienlin, and Leonard Reinecke. 2014. Risky behaviors: How online experiences influence privacy behaviors. In *Von Der Gutenberg-Galaxis Zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy. Surveying old and new frontiers after 50 years of DGPuK*, ed. Birgit Stark, Oliver Quiring, and Nikolaus Jackob, 225–246. Wiesbaden: UVK.

Trepte, Sabine, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. do people know about privacy and data protection strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS). In *Reforming European Data Protection Law*, ed. Serge Gutwirth, Ronald Leenes, and Paul de Hert, 333–366. Dordrecht: Springer.

Trepte, Sabine, and Leonard Reinecke. 2011. The social web as a shelter for privacy and authentic living. In *Privacy online. Perspectives on privacy and self-disclosure in the social web*, ed. Sabine Trepte, and Leonard Reinecke, 143–156. Berlin: Springer.

Tufekci, Zeynep. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* 28(1): 20–36.

Vitak, Jessica. 2012. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media* 56(4): 451–470.