

Sociotechnical Privacy

Mapping the Research Landscape

Carsten Ochs

Technical University Darmstadt

Petra Ilyes

Goethe University Frankfurt

Abstract While it is extraordinarily difficult to theoretically specify privacy, in the last 100 years or so (social) psychology, philosophy, communication studies, economics, and, to a lesser degree, also sociology and anthropology, provided attempts to conceptualize its meaning. Be that as it may, from the 1960s onwards privacy discourse has focused upon data, understood as “personal information”, to a certain extent because of the advent of huge databases and information and communication technologies (ICTs). Influential scholarship at the present time tends to conceive of ICT-related privacy in terms of the “sociotechnical”, thus highlighting the interlocking of human and technical agency. Although having developed a manifold of instruments to research sociotechnical phenomena, STS engagement with sociotechnical privacy, so far, has been rather low-key. In our contribution we therefore provide a mapping of the research landscape, identify connecting factors between STS and sociotechnical privacy research, and calling for further STS contributions.

Keywords: Privacy Theory; Sociotechnical Privacy; Quantitative Privacy Research; Qualitative Privacy Research; STS Privacy Research.

Corresponding author: Carsten Ochs, European Center for Security and Privacy by Design (EC SPRIDE), Technical University Darmstadt, Mornewegstr. 32, 64293 Darmstadt, Germany. Phone: +49 6151 - 16-75427 – Email: carsten.ochs@ec-spride.de

Privacy rhetoric often focuses on the individual (...) Models that go beyond the individual often focus on groups (...) or articulated lists of others (...) But what are the implications of privacy in a networked world where boundaries aren't so coherently defined and when entities aren't so easily articulated?

danah boyd (2013), *Networked Privacy*

I. Introduction

Conceptual work on privacy regularly starts out from the premise that it is extraordinarily difficult to theoretically specify the subject matter.

One of the most thorough accounts of privacy is offered by legal scholar Daniel J. Solove (2008, 1) who states in his seminal *Understanding Privacy* that: “Privacy (...) is a concept in disarray. Nobody can articulate what it means”. A closer look at the academic discourse regarding privacy very quickly demonstrates, however, that this conceptual disarray is not at all due to a lack of analytic engagement. Although one cannot but realize a certain “under-theorisation of the private in sociological thought” (Bailey 2000, 382), “much ink has been spilled in trying to clarify its meaning” (Posner 1978, 393). The discourse on privacy, in other words, in the last hundred years or so,¹ has been proliferating, with a whole range of disciplines, such as legal studies, (social) psychology, philosophy, communication studies, and economics participating in the debate, aiming to contribute to an understanding of the concept of privacy².

A major reason for the difficulty in tackling the privacy problem certainly lies in the multiplicity of dimensions the term refers to: bodily physicality (intimacy; cfr. Inness 1992), material or immaterial resources (private property; cfr. Posner 1978), space (private sphere; cfr. Rössler 2001), freedom of decision (decisional privacy, *ibid.*), as well as institutionalized social domains that are (or are deemed to be) free from public authorities' interventions (the whole of society as private sphere with the State not being authorized to interfere at will, cfr. Habermas 1962), may be designated as “private.” Another dimension the privacy discourse has focused upon from the 1960s onwards is data, understood as “personal information” (cfr. Westin 1970). To a certain extent because of the advent of huge data bases and information and communication technologies (ICTs) initially only at the disposal of government authorities, scholars, over the last several decades, have increasingly explored the status of privacy in face of the massive digitization of vast spheres of social, political, economic life (Westin 1970; Gandy 1993; Garfinkel 2000)³. The resulting, at times rather dystopian, work demonstrates beyond doubt that privacy, to a considerable degree, has become a matter of information flows, and of the technical workings of data processing machines that (in part, but decisively) shape these flows (Nissenbaum 2010). Given that privacy is furthermore a collective achievement (Simmel 1906; Goffman 1973), and thus (perhaps contrary to intuition) not about isolated individuals, but, rather, a social phenomenon, it is appropriate to speak of *sociotechnical*

¹ One might locate the starting point in 1890, beginning with Warren and Brandeis' infamous “The Right to Privacy” (Warren and Brandeis 1890).

² And, despite Bailey criticizing sociology's lack of interest in privacy, there are, indeed, useful contributions current debates repeatedly refer to, such as Simmel (1906), Goffman (1973), and Arendt (1958).

³ At the same time, the neighboring research field of surveillance studies has developed (cf. Lyon 1994). Some scholars consider privacy and surveillance as concepts that need to be distinguished (Stalder 2002), while others seem to somewhat fuse both of them (Marx/Muschert 2007).

privacy when it comes to technologically-mediated, data-driven informational processes (cfr. again Nissenbaum 2010). Accordingly, research on privacy with respect to new, digital data-collecting and processing technologies in distributed, networked computational environments must acknowledge privacy's recent sociotechnical entanglements or dynamic, heterogeneous associations.⁴ On this note, Friedewald and Pohoryles, for example, state that: "Technology and privacy are two intertwined notions that must be jointly analysed" (2013, 1).

This is even more true, given that, since the 1990s, sociotechnical privacy has been significantly transformed, again, with the advent of the Internet and the World Wide Web; with the advent of "smart" cards, meters, grids, and homes; with the advent of "virtual" bank accounts and online banking; with the advent of digital navigation through analogous space; with the advent of social media such Online Social Networks (OSNs) for communication and networking, and Business-to-Consumers (B2C) E-Commerce for purchasing and selling goods online. In this paper, we focus on mapping the research landscape of the latter two, both of which involve forms of sociotechnical privacy. The reason for this focus is that, at present, privacy and privacy breaches in OSNs and E-Commerce environments are a major subject in academic research, and also are at the core of the background for staging public policy debates on privacy.

The "sociotechnical" is a classic concept in Science and Technology Studies (STS) (e.g. Akrich 1994, 1989; Bijker and Law 1992; Callon 2004; Law 2000). It denotes the interplay in highly complex situations of technological infrastructures and practices, of social and material agencies, involving a wide array of heterogeneous actors – human and non-human or technical and non-technical – engaged in numerous controversies. Sociotechnical privacy as a concept, therefore, is perfectly suited for STS. We are aware, of course, that STS is a highly contentious field, and that there is no "solid" definition of it (Coopmans *et al.* 2004, 2). However, since the 1980s, the label STS is most commonly used for designating (social) constructivist and post-constructivist research on science and technology, albeit not in a binding or consistent way (Ilyes 2006). However, technology "as an object of inquiry" in STS is generally conceptualized "in terms of an ensemble of social and material elements in which dynamic combinations of determination and contingency generate different sociomaterial configurations" (Boczkowski and Lievrouw 2008, 957). In this sense, a purely technological or tool understanding of the complex, interactive systems that involve sociotechnical privacy falls short of their deep embeddedness and situatedness in, or entanglement with, social (or cultural) contexts (e.g. Akrich 1994; MacKenzie and Wajcman 1999). As we will explain in the conclusion, it is this general insight which renders the con-

⁴ Ellison and boyd (2013, 166) define sociotechnical systems as systems in which "social and technical factors shape one another".

ceptual tools and methodological instruments of STS fruitful for research on sociotechnical privacy.

Having said that, we would like to clarify that whereas STS engagement with sociotechnical privacy so far has been rather low-key, the research landscape concerning this form of privacy is much more extensive and diverse than we are able to illustrate on the pages to come. What is more, being located at German research institutions we approach the international research landscape from where we are based, which is why our mapping will predominantly focus on German, European and United States research. For these reasons the map that we draw will be somewhat selective; however, we presume this to be negligible for the argument presented here since our main interest lies in unlocking connecting factors between sociotechnical privacy research and STS, and we assume that our selective mapping is appropriate for our particular concern. So the paper proceeds as follows: in the next paragraph we will offer a rough overview over quantitative studies dealing with sociotechnical privacy in the last ten years or so (1); thereupon we will attempt to map the inventory of qualitative research in this area (2); finally, we will flesh out three possible STS contributions to sociotechnical privacy studies (3).

2. Quantitative Research on Sociotechnical Privacy

Some of the earliest and to date most influential quantitative research on sociotechnical privacy in OSNs and B2C E-Commerce stems from the fields of behavioural economics, communication studies and (media) psychology. This research mostly centres on the idea of individual actors, often conceived of as consumers, who make individual privacy decisions (as explained in Gürses and Diaz 2013, 6); in so doing, these individuals are deemed to trade personal information off for (economic or social) benefits. Behavioural economists Alessandro Acquisti and Jens Grossklags formulated the *leitmotif* of this kind of approach as early as 2003 by identifying “a dichotomy between stated attitudes and actual behavior of individuals facing decisions affecting their privacy and their personal information security” (Acquisti and Grossklags 2003, 1). Those individuals are generally deemed to make rational decisions (Acquisti and Grossklags 2005), therefore research strategies aim to compare users' rational valuation of privacy in online environments with the information they actually reveal via profiles, postings, and so on. A behavioral economics research strategy proceeds by interrogating users, with the help of surveys, on the value they assign to personal information. Additionally, profile data and similar data made available by users in OSNs are collected, examined, and tested for a match or mismatch between attitudes stated in the surveys, and actual profile settings (cf. Gross and Acquisti 2005; Acquisti and Gross 2006). More often than not researchers found a discrepancy

between both. The term coined for this mismatch was “Privacy Paradox” (Barnes 2006).

Research along these lines attempted to identify a series of issues, among them (1) privacy concerns and the trust that users assign to certain OSNs (Dwyer *et al.* 2007); (2) users' perceptions of “benefits” (i.e. social capital) of OSNs for them (cf. Ellison *et al.* 2007; Ellison *et al.* 2011; Stutzman *et al.* 2012a); (3) information protection strategies in OSNs, and the growing awareness of, privacy issues as well as techniques to limit unintended dissemination of information (Tufekci 2008; Young and Quan-Haase 2009; Stutzman and Kramer-Duffield 2010); (4) the cultural shaping of privacy concerns (Wang *et al.* 2011a); (5) the change in use and perception of OSNs over time (Lampe *et al.* 2008; boyd and Hargittai 2010; Stutzman *et al.* 2012b); and (6) whether and how OSN use affects self-disclosure (Trepte and Reinecke 2013).

Many of these studies were concerned with what was perceived as a discrepancy between stated attitudes and actual disclosure practice in OSNs. In the same vein, early research in the realm of E-Commerce detected a similar dichotomy (e.g. cfr. Berendt *et al.* 2005). As the objective of many of these studies is to inform privacy research in computer science (e.g. on Privacy-Enhancing Technologies, abbreviated PETs) the central question is how to account for this discrepancy and find a design solution. One major approach is the so-called “soft paternalism” approach based on the idea of “privacy nudges”, a strategy that works on the premise that users must be nudged by the software into considering the privacy implications of their online actions (Acquisti 2009; Wang *et al.* 2013). For example, studies uncovered that users often regretted having posted a piece of information (Wang *et al.* 2011b). Several suggestions were made and tested. One suggestion was to provide a tool informing users about the audiences for which a post was visible; another one was to introduce time delays to give users the opportunity to reconsider as to whether they wanted to post the message or not; and yet another suggestion was to indicate potentially inappropriate semantics in a post (e.g. swearing; Wang *et al.* 2013). With respect to E-Commerce, researchers experimented with providing tools that indicated the “privacy-friendliness” of online shops, “nudging” users towards financially less attractive but more privacy-friendly services (Tsai *et al.* 2011).

These studies are well suited to take on rather narrowly defined privacy issues on the Internet. However, they rarely consider collective or interactional dimensions of privacy practices (Gürses and Diaz 2013; Dourish and Anderson 2006). In fact, what is termed “practice” in many of these studies, empirically and methodologically only comes to the surface in the form of participants' ticking preformulated statements in a survey. Often such surveys consider “practice” to be the equivalent to individuals' behavior, assuming that it is possible to separate “behavioural bits” (i.e. decontextualized privacy decisions, e.g. when setting up a profile, or similar actions) from users' extended social context. In this view, users

give rational and clear-cut accounts of the reasons motivating those “bits”. It follows from this perspective that it should be possible to identify these reasons by interrogating users with the help of surveys and juxtaposing them with what is held to be the corresponding “actual practice.” In contrast, STS approaches situate practice within the collectivity of sociotechnical “agencements” (Callon 2006), or “social worlds” (Clarke and Star 2008). Empirically and analytically, user practices cannot be studied in isolation from those collectivities. In order to capture user practices *in situ* qualitative approaches are necessary.

3. Qualitative Research on Sociotechnical Privacy

There is to date a considerable number of studies on privacy issues in technically mediated environments employing both a sociotechnical approach, and a qualitative and mixed-method approach to investigate users' privacy management and sharing practices in OSNs (e.g. Besmer *et al.* 2010; boyd 2007; Brandtzaeg *et al.* 2010; Cunningham and Masoodian 2010; Dowd 2011; Fowley 2011; Lampinen *et al.* 2011; Lange 2007; Rotman *et al.* 2012a; Nippert-Eng 2007; Sleeper *et al.* 2013; Viseu *et al.* 2004). These investigations are qualitative (or partly qualitative) user studies conducted in a range of fields such as HCI (Human-Computer Interaction) and CSCW (Computer-Supported Cooperative Work).⁵

There are also some full-fledged ethnographies on OSNs that have become quite influential. danah boyd, for example, in 2008 brought forward an impressive study of US American Teens' use practices in a range of OSNs (or social network sites, abbreviated SNS, as she prefers to call them) (2008b). Moreover, not only did she provide, together with Nicole B. Ellison, what is the standard definition of OSNs (boyd and Ellison 2007), she also developed the widely-used analytical concept of “networked publics” to capture the characteristics of OSNs (boyd 2008). Interestingly, by doing fieldwork, boyd (2011) did not simply offer common explanations of a say-this-but-do-that type of user, but, instead, was able to empirically demonstrate that the users she observed (US Teens) in no way rejected privacy as a value, as it is often claimed (cfr. the debate on the “privacy paradox”) Rather, they had the normative expectation that certain classes of actors, such as parents or teachers, were simply not authorized to “sniff out” personal information; doing so was considered a privacy breach, just like reading someone's diary without their consent (boyd 2011). The reason for the occurrence of the so called privacy para-

⁵ HCI and CSCW researchers have employed ethnographically informed approaches since decades, particularly to gain insights into actual practices of users of computational environments in workplaces (cfr. Anderson 1996; Crabtree *et al.* 2006; Dourish 2001; Hughes 1995; Viller and Sommerville 2000).

dox, therefore, was not so much attributable to discrepancies between stated attitudes and actual behaviour as to a clash of normative assumptions, as well as to power asymmetries in terms of options to achieve “contextual integrity” (Nissenbaum 2004).

Other qualitative studies on privacy issues in OSNs similarly help to differentiate the specific forms privacy (and privacy practices) take on in online environments. Based on an ethnography of Facebook users, Raynes-Goldie (2010), for example, distinguishes between “institutional privacy”, i.e. privacy matters to do with access of providers and third parties to users' personal information (which can hardly be controlled by users), and “social privacy”, i.e. privacy matters to do with users' privacy management *vis-a-vis* other users (which is potentially controllable by users with the help of privacy settings provided by OSNs). Raynes-Goldie holds that, typically, teenagers do care less for “institutional privacy”, compared to “social privacy.”⁶

Despite of drawing on rather small sample sizes, qualitative and ethnographic studies on actual user practices allow a more nuanced perspective on privacy in technically mediated environments. Insights into actual user practices may point to possible solutions for mitigating problems of unauthorized data access, and thus to suggest ways of giving users more control over their privacy settings or to make it easier for users to manage them (Beye *et al.* 2010, 13). In fact, as far as the design of online interactive systems is concerned, bringing an understanding of the social to the research of these systems, and conceiving of them as sociotechnical (or “technosocial”) ensembles rather than just technical tools has become a widely adopted perspective. Many scholars in the field of systems design now emphasize anthropological and sociological methodological approaches in order to provide insights into situated and contextualized end users' information practice, i.e. how they manage their activities and security on an everyday, practical basis (cfr. Dourish 2001, 2004; Dourish *et al.* 2004; Dourish and Anderson 2006). Rotman *et al.* (2012), for instance, argue that quantitative methods have only a limited capacity for exploring why people do something online. Ethnographers, they suggest, may uncover implicit meanings and new behaviours by conducting in-depth research in natural settings (Rotman *et al.* 2012b). Sociotechnical approaches are, in fact, employed within the field of systems design (e.g. Sutcliffe 2000; Goggins *et al.* 2011; Mostashari and Sussman 2009), but – with very few exceptions – work in this field makes no reference to STS nor does it employ qualitative user studies.

The latter observation applies to research on sociotechnical privacy in general: studies locating themselves explicitly within the STS field, taking up STS conceptual tools are pretty rare. Here are some of those that do

⁶ Other scholars prefer the terms “interpersonal” (Palen and Dourish 2003; Johnson *et al.* 2012) or “interactional” privacy (Lipford *et al.* 2012; Wisniewski 2011).

so: Ochs and Löw apply some of the STS instruments to pursue their more general interest in possibilities of building a “culture of trust” on the Internet including the matching of techno-legal infrastructures, fair information practices and user competences (Ochs and Löw 2012). Van der Velden and Emam (2012) focus on understanding actual privacy-protection techniques of long-term or chronically ill teenagers using social media. Ochs (2013) analytically juxtaposes empirically identified normative scripts shaping users' agency with the cookie script harnessed for targeted advertisement, thus demonstrating the emergence of intrinsically contradictory information practices. Still further in empirically integrating the non-human shaping of sociotechnical privacy go Poller *et al.* (2013). Their work is based on a collaboration between computer scientists and cultural anthropologists using both self-reported data and technically elicited *in situ* data from OSNs to achieve a better understanding of actual user practices and user interactions. By analyzing users' interaction with other users as well as with technology, they aim at making valid suggestions for a more user-friendly software design of OSNs.

In fact, systematically including non-human actors' role – be they technical, legal, or other – in the shaping of sociotechnical privacy is what is urgently required in privacy research. Gürses and Diaz (2013) plausibly argue for an integration of “surveillance perspectives” and “social perspectives”, i.e. of what we have called above “institutional privacy” and “social privacy.” To understand sociotechnical privacy, in other words, it is mandatory that we account for the wider sociotechnical ensemble or “agencement”: users, preferences, infrastructures, providers, technology, laws, etc. Recent research, quantitative as well as qualitative one, has begun to pick up on this insight, including providers and technologies in the research design. Stutzman *et al.* (2012), for example, combined their quantitative longitudinal study of Facebook use by undergraduates at a US University with a qualitative analysis of Facebook privacy settings during the course of the study to explain some of their findings. Raynes-Goldie empirically investigated both OSN users and the provider (Facebook Inc.) to demonstrate that: “Facebook Inc. plays a critical, yet often overlooked role in shaping privacy norms and behaviours through site policies and architecture” (Raynes-Goldie 2012, ii).

Mapping the landscape of sociotechnical privacy research eventually reveals that there is a need to be more inclusive, i.e. to take into account the various heterogeneous actors / agencies shaping privacy practices and shaped by them. This requirement has already been acknowledged for some time within privacy research in general. We argue that STS is perfectly equipped to contribute to this task. So in the remainder of the paper we will suggest how STS may contribute to exploring sociotechnical privacy.

4. Three Possible STS Contributions to Studying Sociotechnical Privacy

Studying online social media on the Internet (such as Facebook, YouTube, Orkut, Twitter, Flickr, Google+, Pinterest, etc.) is a hot topic for researchers from different disciplines. There is hardly any doubt that these media have changed the way the Internet is being used, and that the implications of these changes are not well understood, particularly with respect to privacy and security issues. Increasingly, researchers articulate the need to study these technologically mediated online environments from various perspectives⁷. However, STS has not yet seriously engaged with sociotechnical privacy on the Internet. Although STS programs at universities often emphasize that privacy in technically mediated environments is a central public issue that should be investigated from an STS perspective,⁸ few studies have visibly materialized so far⁹. Whereas the theme of surveillance was present to a certain extent at recent STS conferences¹⁰, the question of managing privacy in online social networks by their users was hardly touched¹¹. We want to argue, however, that STS with its characteristic non-essentialist and mutual-shaping stance will be able to contribute to research on sociotechnical privacy. We want to particularly suggest three points.

4.1. Situated Actions and Practices

A first move of STS-informed research on sociotechnical privacy would be to step back from given definitions, and to follow agencies as they co-constitute the ontologies of privacies in processes of unfolding in different sociotechnical arrangements or “agencements”. Therefore, STS first contribution would be to take privacy not as a given, but to investigate into sociotechnical (or “technosocial”) entanglements, i.e. the co-constitution or social shaping of technology by heterogeneous actors or agencies. OSN users' actions are part of wider-ranging sociotechnical practices involving communication, networking and so on, that is, in STS

⁷ For instance, recently, at the Second International Workshop on Privacy and Security in Online Social Media, co-located with WWW 2013, May 14, 2013, Rio De Janeiro, Brazil.

⁸ Two cases are STS at MIT and Cornell University.

⁹ There is some work in STS on other aspects of social media, e.g. on ethical questions, but not necessarily qualitative studies (cf. e.g. Light *et al.* 2008).

¹⁰ For instance, at three panels at the 4S/EASST Joint Conference 2012 Copenhagen.

¹¹ Two of the few presentations at the 4S/EASST Joint Conference 2012 that did touch this point are by Maja van der Velden and Andreas Poller and Andreas Kramm.

terms, they are “situated” actions.¹² As a consequence, when we deal with a subject that is socially and culturally as loaded as privacy, it seems hardly possible to sever the informational dimension of privacy from its ties to dimensions of intimacy, property, freedom of choice, and so on. Additionally, it is quite probable that conceptualizations of privacy vary with respect to the given social setting under scrutiny. So, instead of portraying privacy as a matter of purely individual behavior, or as something essential, equipped with inherent features, it is more appropriate to investigate (a) into what privacy means in different social worlds to different actors; (b) how the latter relate to different taken-for-granted values, norms, ideas, interests, etc.; (c) how they aim to inscribe these into material structures, given the asymmetric distribution of capacities to do so; and (d) how different notions clash, thus destabilizing discursive, semantic, semiotic, and material dimensions. Furthermore, situated actions and practices are not only produced by those who use some online service, but also by those providing it, including the material agents shaping the flow of information, and others, e.g. regulatory agencies. It may be the case that within such complex constellations there are countervailing “scripts” (Akrich 1994) shaped by quite different norms and values. Still however, insofar as the contradictions do not necessarily become visible, and consequently do not play out, all the agents together might build networks producing practices. For example, users may operate with normative assumptions not matching the technological scripts that shape the flow of information; however, without being aware of it, so in spite of their norms being somewhat violated, they still develop practices in OSNs. Hence, what seems a paradox at first glance might, in fact, surface as a matter of asymmetric translation processes rather than of inconsistency: users may simply not be able to make *their* scripts part of the program running. To sum up, studying situated privacy practices would make the simultaneous fluidity (no once-and-for-all privacy-in-society) and robustness (relatively stable patterns of privacy practices in different social worlds) – that is, the contingencies and regularities of sociotechnical privacy – visible.

4.2. Heterogeneous Actors

We argue that this approach requests us to identify connected sites and stabilizing mechanisms, trace a network and account for how the association is held together (Latour 2005). While keeping an eye on the users, we must also turn the lens somewhat away from them and also include other entities. STS user studies do not only look at users' roles in

¹² The concept of “situated action” has been introduced by Lucy Suchman (1987) to the debate on technical design, and has become a central concept in STS.

technological development and innovation but also at the complex interplay of users and artifacts (cfr. Oudshoorn and Pinch 2008). This perspective points to emergent properties, unintended consequences and co-evolutionary dynamics of technical artifacts (cf. e.g. Akrich 1994; Callon 1987). STS emphasizes that there are no “correct” uses of a given technological artifact, only intended, recommended, expected or dominant ones (Aibar 2010, 179). Users do not necessarily “come forward to play the roles envisaged by the designers” (Akrich 1994, 208), but come up with new and surprising uses. Indeed, qualitative, ethnographically informed studies on sharing strategies of OSN users demonstrate that users often do not fully grasp how the system technically functions. They also show that users invent strategies and workarounds instead of using built-in functions (e.g. boyd and Marwick 2011; Poller *et al.* 2013). In this sense, unsurprisingly, users still play an integral part in sociotechnical privacy studies. If we want to come to terms with how practices are collectively produced, however, we quite obviously have to deal not only with users, but also with technologies, designers, providers, shareholders, privacy advocates, regulators, laws, government authorities, global governance agencies, etc., all of them participating in the shaping of practices, attempting to introduce scripts in order to make programs of action run. Sociotechnical privacy may be produced as much by data regulation laws as by users' ideas and actions; it may be shaped by the business models of the Web 2.0 industry just as much as by public discourses on the risks of “social media”; and it may be configured by technical functionalities just as much as by the semantics and semiotics of presenting them to users. We posit, therefore, that the second contribution of STS is to account for all these entities without privileging any of them a priori, but to rather empirically determine their relevance.

4.3. Ethnographically Informed Studies

While the merits of an ethnographically informed approach are obvious, what rains on its parade is that such an endeavour threatens to run into considerable methodological challenges (e.g. Rotman *et al.* 2012; Gürses and Diaz 2013). For instance, on-site observations of user practices in OSNs or on E-Commerce sites can be difficult because unlike in studies implying a physical site, researchers in online environments cannot simply go and visit some place, and observe users *in situ*. Therefore, in addition to classical qualitative research methods, the deployment of software-supported research techniques may be helpful (e.g. experience sampling, embedded comment tools, activity logs, etc.) to collect qualitative, contextualized *in situ* data.

Another case in point is access to providers' data. Gürses and Diaz point out that in practice it is not possible to observe how providers make

management decisions, nor are the algorithms that shape the flow of information visible. In other words, providers' practices – both human and nonhuman ones – are anything but transparent, and in this sense the “opacity of OSN providers” poses considerable challenges for research in PETs as well as in sociotechnical privacy (Gürses and Diaz 2013, 7). Problems such as these are, of course, not unique to studying sociotechnical privacy but also arise in other fields of STS when corporate interests (e.g. algorithmic financial markets) and other high-level interests (e.g. political decision making) are at stake. Some research draws on alternative strategies, analyzing reverse engineering of the system; public statements of enterprises; the legal framework of services, and so on. However, these strategies often require to establish alliances and collaborations with other disciplines, such as computer science, legal studies, economics, etc. In spite of the methodological challenges we argue that by investigating into actual practices and situated action, STS-informed research may both provide viable suggestions for better privacy solutions, and a better understanding of sociotechnical privacy in emergent systems; for, if anything, STS scholars have proven in the course of the last decades time and again that they are capable of building alliances with other fields and disciplines; and, what is more, that they are not easy to intimidate when it comes to researching fields which are difficult to study. Thus, the third contribution of STS to researching sociotechnical privacy is the doggedness it has acquired over the years.

Let's take up the challenge!

References

- Acquisti, A. (2009) *Nudging Privacy. The Behavioral Economics of Personal Information*, in “IEEE Security & Privacy”, (7) 6, pp. 82-85.
- Acquisti, A. and Gross, R. (2006) *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, in G. Danezis and P. Golle (eds.), *Privacy Enhancing Technologies*, 6th International Workshop PET 2006, Berlin and Heidelberg, Springer, pp. 36-58.
- Acquisti, A. and Grossklags, J. (2003) *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior*. 2nd annual Workshop on Economics and Information Security, in http://www.cpppe.umd.edu/rhsmith3/papers/Final_session6_acquisti.grossklags.pdf (retrieved September 5, 2013).
- Acquisti, A. and Grossklags, J. (2005) *Privacy and Rationality in Individual Decision Making*, in “IEEE Security & Privacy”, 3 (1), pp. 26-33.
- Aibar, E. (2010) *A Critical Analysis of Information Society – Conceptualizations from an STS Point of View*, in “TripleC”, 8 (2), pp. 177-182.
- Akrich, M. (1989) *La construction d'un système socio-technique. Esquisse pour une*

- anthropologie des techniques*, in “Anthropologie et Sociétés”, 13 (2), pp. 31-54.
- Akrich, M. (1994) *The De-Description of Technical Objects*, in W.E. Bijker and J. Law (eds.), *Shaping Technology / Building Society: Studies in Sociotechnical Change*, Cambridge, MA, MIT Press, pp. 205-224.
- Anderson, B. (1996) *Work, Ethnography and System Design*, in *Rank Xerox Research. Centre Technical Report EPC-1996*, Rank Xerox Research Centre, Cambridge.
- Arendt, H. (1958) *The Human Condition*, Chicago, University of Chicago Press.
- Bailey, J. (2000) *Some Meaning of 'the Private' in Sociological Thought*, in “Sociology”, 34 (3), pp. 381-401.
- Barnes, S. (2006) *A Privacy Paradox: Social Networking in the United States*, in “First Monday”, 11 (9).
- Berendt, B., Günther, O. and Spiekermann, S. (2005) *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, in “Communications of the ACM”, 48 (4), pp. 101-106.
- Besmer, A. and Richter Lipford, H. (2010) *Moving beyond untagging: photo privacy in a tagged world*, in E.D. Mynatt, D. Schoner, G. Fitzpatrick, S.E. Hudson, W.K. Edwards and T. Rodden (eds.), “CHI”, pp. 1563-1572.
- Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R. and Tang, Q. (2010) *Literature Overview – Privacy in Online Social Networks*, in “Technical Report TR-CTIT-10-36”, Centre for Telematics and Information Technology University of Twente, Enschede.
- Bijker, W.E. and Law, J. (eds.) (1992) *Shaping Technology/Building Society. Studies in Sociotechnical Change*, Cambridge, MA, MIT Press.
- Boczkowski, P. and Lievrouw, L. A. (2008) *Bridging STS and Communication Studies: Scholarship on Media and Information Technologies*, in E.J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (eds.), *Handbook of Science and Technology Studies*, Cambridge, MA, MIT Press, pp. 951-977.
- boyd, d. (2007) *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, in D. Buckingham (ed.), *Youth, Identity, and Digital Media*, Cambridge, MA, MIT Press, pp. 119-142.
- boyd, d. (2008) *Taken Out of Context: American Teen Sociality in Networked Publics*, PhD Dissertation, University of California-Berkeley, School of Information, <http://www.danah.org/papers/TakenOutOfContext.pdf>, retrieved August 29, 2013.
- boyd, d. (2011) *Living in a Publicity World: Privatsphäre und Öffentlichkeit in sozialen Netzwerken*, in Heinrich-Böll-Stiftung (ed.), *#public life. Digitale Intimität, die Privatsphäre und das Netz*, Berlin, agit-druck, pp. 28-35.
- boyd, d. (2013) *Networked Privacy*, in “Surveillance & Society”, 10 (3/4), pp. 348-350.

- boyd, d. and Ellison, N.B. (2007) *Social Network Sites: Definition, History, and Scholarship*, in "Journal of Computer-Mediated Communication", 13 (1), pp. 210-230.
- boyd, d. and Hargittai, E. (2010) *Facebook's Privacy Settings: Who Cares?*, in "First Monday", 15 (8).
- boyd, d. and Marwick, A. (2011) *Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies*, in *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011*. <http://ssrn.com/abstract=1925128>, retrieved September 4, 2013.
- Brandtzaeg, P.B., Lüders, M. and Skjetne, J.H. (2010) *Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites*, in "International Journal of Human-Computer Interaction, Special Issue: HCI and Social Computing", 26 (11-12), pp. 1006-1030.
- Callon, M. (1987) *Society in the Making: The Study of Technology as a Tool for Sociological Analysis*, in W.E. Bijker, T. Hughes, and T. Pinch (eds.), *The Social Construction of Technological Systems*, Cambridge, MA, MIT Press, pp. 83-193.
- Callon, M. (2004) *The role of hybrid communities and socio-technical arrangements in the participatory design*, in "Journal of the Center for Information Studies", 5, pp. 3-10.
- Callon, M. (2006) *What does it mean to say that economics is performative?* in "CSI Working Papers Series", No. 5.
- Clarke, A.E. and Star, S.L. (2008) *The Social Worlds Framework: A Theory/Methods Package*, in E.J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (eds.), *The Handbook of Science and Technology Studies*, Cambridge MA, MIT Press, pp. 113-137.
- Coopmans, C., Neyland, D. and Woolgar, S. (2004) *Does STS mean business? – some issues and questions*, workshop at Saïd Business School, University of Oxford, June 30.
- Crabtree, A., Benford, S., Greenhalgh, C., Tennent, P., Chalmers, M. and Brown, B. (2006). *Supporting ethnographic studies of ubiquitous computing in the wild*, in "Proceedings of the 6th conference on Designing Interactive systems", New York, pp. 60-69.
- Cunningham, S.J. and Masoodian, M. (2010) *Analyzing users' behaviour to identify their privacy concerns*, paper presented at Workshop on Privacy and Usability Methods Pow-wow (PUMP) 2010, Dundee, Scotland, September, 6.
- Dourish, P. (2001) *Where the Action Is. The Foundation of Embodied Interaction*. Cambridge, MA, MIT Press.
- Dourish, P. (2004) *What We Talk About When We Talk About Context*, in "Personal and Ubiquitous Computing", 8 (1), pp. 19-30.
- Dourish, P. and Anderson, K. (2006) *Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena*, in "Human-Computer Interaction", 21, pp. 319-342.

- Dourish, P., Grinter, R.E., Delgado De La Flor, J. and Joseph, M. (2004) *Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem*, in "Personal and Ubiquitous Computing", 8 (6), pp. 391-401.
- Dowd, M. (2011) *Contextualised concerns: The online privacy attitudes of young adults*, in *Privacy and Identity Management for Life*, "IFIP Advances in Information and Communication Technology", Volume 352, Springer, pp. 78-89.
- Dwyer, C., Hiltz, S. and Passerini, K. (2007) *Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace*, in "AMCIS 2007 Proceedings. Paper 339".
- Ellison, N. B. and boyd, d. (2013) *Sociality through social network sites*, in Dutton, W.H. (ed.), *The Oxford Handbook of Internet Studies*. Oxford, Oxford University Press, pp. 151-172.
- Ellison, N. B., Steinfield, C. and Lampe, C. (2007) *The "Benefits" of Facebook-Friends: Social Capital and College Students' Use of Online Social Network Sites*, in "Journal of Computer-Mediated Communication", 12, pp. 1143-1168.
- Ellison, N. B., Vitak, J., Steinfield, C., Gray, R. and Lampe, C. (2011) *Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment*, in S. Trepte, S. and L. Reinecke (eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, New York, Springer, pp. 19-32.
- Fowley, C. (2011) *Publishing the confidential. An ethnographic study of young Irish bloggers*, PhD Thesis, Dublin City University.
- Friedewald, M. and Pohoryles, R.J. (2013) *Technology and privacy*, in "Innovation: The European Journal of Social Science Research", 26 (1-2), pp. 1-6.
- Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder/CO, The Westview Press.
- Garfinkel, S. (2000) *Database Nation: The Death of Privacy in the 21st Century*, Beijing, O'Reilly.
- Goffman, E. (1973) *The Presentation of Self in Everyday Life*, New York, The Overlook Press.
- Goggins, S. P., Laffey, J. and Gallagher, M. (2011) *Completely online group formation and development: small groups as socio-technical systems*, in "Information Technology & People", 24 (2), pp. 104-133.
- Gross, R. and Acquisti, A. (2005) *Information Revelation and Privacy in Online Social Networks (The Facebook Case)*, in "Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society", pp. 71-80.
- Gürses, S. and Diaz, C. (2013) *Two Tales of Privacy in Online Social Networks*, in "IEEE Security & Privacy", 11 (3), pp. 29-37.
- Habermas, J. (1962) *Strukturwandel der Öffentlichkeit, Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*, Neuwied, Luchterhand.

- Hughes, J. (1995) *The Role of Ethnography in Interactive Systems Design*, in "Interactions", 2 (2), pp. 57-65.
- Ilyes, P. (2006) *Zum Stand der Forschung des englischsprachigen "Science and Technology" (STS)-Diskurses*, in "Teilstudie im Rahmen des Forschungsprojekts 'Computersimulationen – Neue Instrumente der Wissensproduktion' im Rahmen der BMBF Initiative Wissen für Entscheidungsprozesse. Forschung zum Verhältnis von Wissenschaft, Politik und Gesellschaft".
- Inness, J. (1992) *Privacy, Intimacy, and Isolation*, Oxford, Oxford University Press.
- Johnson, M., Egelman, S. and Bellovin, S.M. (2012) *Facebook and Privacy: It's Complicated*, in "Symposium on Usable Privacy and Security (SOUPS) 2012", July 11–13, Washington.
- Lampe, C., Ellison, N.B. and Steinfield, C. (2008) *Changes in use and perception of Facebook*, in "Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW '08). ACM, New York", pp. 721-730.
- Lampinen, A., Lehtinen, V., Lehmuskallio, A. and Tamminen, S. (2011) *We're in It Together: Interpersonal Management of Disclosure in Social Network Services*, in "CHI 2011, Session: Privacy May 7-12, 2011, Vancouver, BC, Canada".
- Lange, P. G. (2007) *Publicly Private and Privately Public: Social Networking on Youtube*, in "Journal for Computer-Mediated Communication", 13 (1), pp. 361-380.
- Latour, B. (2005) *Reassembling the Social. An Introduction to Actor-Network-Theory*. Oxford, Oxford University Press.
- Law, J. (2000) *Networks, Relations, Cyborgs: on the Social Study of Technology*, in "Centre for Science Studies, Lancaster University Working Paper Series". <http://www.lancaster.ac.uk/sociology/research/publications/papers/law-networks-relations-cyborgs.pdf>, retrieved November 21, 2013.
- Light, B., McGrath, K. and Griffiths, M. (2008) *More Than Just Friends? Facebook, Disclosive Ethics and the Morality of Technology*, in "Twenty Ninth International Conference on Information Systems, Paris 2008. ICIS 2008 Proceedings", Paper 193.
- Lipford, H.R., Wisniewski, P., Lampe, C., Kisselburgh, L. and Caine, K. (2012) *Reconciling Privacy with Social Media*, in "Proceedings of the 2012 ACM Conference on Computer Supported Corporative Work Companion", pp. 19-20.
- Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*, Cambridge, Polity Press.
- MacKenzie, D., and Wajcman, J. (1999) *Introductory essay: the social shaping of technology*, in D. MacKenzie, D. and J. Wajcman (eds.), *The Social Shaping of Technology*, Buckingham, Open University Press, pp. 3-27.
- Marx, G.T. and Muschert, G. (2007) *Personal Information, Borders, and the New Surveillance Studies*, in "Annual Review on Law and Social Science", 3, pp. 375-395.

- Mostashari, A. and Sussman, J.M. (2009) *A Framework for Analysis, Design and Management of Complex Large-Scale Interconnected Open Sociotechnological Systems*, in "International Journal of Decision Support System Technology (IJDSST)", 1 (2), pp. 53-68.
- Nippert-Eng, C. (2007) *Privacy in the United States: Some Implications for Design* *Privacy in the United States*, in "International Journal of Design", 1 (2), pp. 1-10.
- Nissenbaum, H.F. (2004) *Privacy as Contextual Integrity*, in "Social Science Research Network Working Paper Series", May.
- Nissenbaum, H.F. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, CA, Stanford University Press.
- Ochs, C. (2013) *Wettrüsten der Skripte: Widersprüchlichkeiten soziotechnischer Privatheitspraktiken im Internet*, in U. Ackermann (ed.), *Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter*, Frankfurt/M., Humanities Online, pp. 111-129.
- Ochs, C. and Löw, M. (2012) *Un/faire Informationspraktiken: Internet Privacy aus sozialwissenschaftlicher Perspektive*, in J. Buchmann (ed.), *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme / amultidisciplinary analysis* (acatech STUDIE), Berlin, Springer, pp. 15-61.
- Oudshoorn, N. and Pinch, T. (2008) *User-Technology Relationships: Some Recent Developments*, in E.J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (eds.), *The Handbook of Science and Technology Studies*, Cambridge, MA, MIT Press, pp. 541-565.
- Palen, L. and Dourish, P. (2003) *Unpacking "privacy" for a networked world*, in "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03). ACM, New York, NY, USA", pp. 129-136.
- Poller, A., Kramm, A. and Ilyes, P. (2013) *Designing privacy-aware online social networks – A reflective socio-technical approach*, in "CSCW '13 Measuring Networked Social Privacy Workshop, February 23-27, 2013, San Antonio, Texas, USA".
- Posner, R. (1978) *The Right of Privacy*, in "Georgia Law Review", 12 (3), pp. 393-422.
- Raynes-Goldie, K. (2010) *Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook*, in "First Monday", 15 (1).
- Raynes-Goldie, K. (2012) *Privacy in the Age of Facebook: Discourse, Architecture, Consequences*, PhD Thesis, Curtin University, Perth/Australia, in http://www.k4t3.org/wpcontent/uploads/2012/09/privacy_in_the_age_of_fac ebook_raynes-goldie.pdf, retrieved September 5, 2013.
- Rössler, B. (2001) *Der Wert des Privaten*, Frankfurt/M., Suhrkamp.
- Rotman, D., Preece, J., He, Y. and Druin, A. (2012a) *Extreme Ethnography: Challenges for Research in Large Scale Online Environments*, in "Proceedings of the 2012 iConference, New York, NY, USA, 2012. ACM", pp. 207-214.

- Rotman, D., Preece, J., Hammock, J., Procita, K., Hansen, D.L., Parr, C., Lewis, D. and Jacobs, D.W. (2012b) *Dynamic changes in motivation in collaborative citizen-science projects*, in S.E. Poltrock, C. Simone, J. Grudin, G. Mark and J. Riedl (eds.), "CSCW", 217-226.
- Simmel, G. (1906) *The Sociology of Secrets and of Secret Societies*, in "American Journal of Sociology", 11 (4), pp. 441-498.
- Sleeper, M., Balebako, R., Das, S., McConahy, A.L., Wiese, J. and Cranor, L.F. (2013) *The Post that Wasn't: Exploring Self-Censorship on Facebook*, in "CSCW13, February 23–27, 2013, San Antonio, Texas, USA".
- Solove, D. J. (2008) *Understanding Privacy*, Cambridge, MA, Harvard University Press.
- Stalder, F. (2002) *Privacy is not the Antidote to Surveillance*, in "Surveillance & Society, 1 (1), pp. 120-124.
- Stutzman, F. and Kramer-Duffield, J. (2010) *Friends Only: Examining a Privacy-Enhancing Behavior in Facebook*, in "CHI 2010: Privacy, April 10–15, 2010, Atlanta, GA, USA".
- Stutzman, F., Vitak, J., Ellison, N.B., Gray, R. and Lampe, C. (2012a) *Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook*, in "Proceedings of the 6th annual International Conference on Weblogs and Social Media (ICWSM). Washington, DC: Association for the Advancement of Artificial Intelligence".
- Stutzman, F., Gross, R. and Acquisti, A. (2012b) *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, in "Journal of Privacy and Confidentiality", 4 (2), pp. 7-41.
- Suchman, L. (1987) *Plans and Situated Actions: The Problem of Human-machine communication*, Cambridge, Cambridge University Press.
- Sutcliffe, A.G. (2000) *Requirements Analysis for Socio-Technical System Design*, in "Information Systems", 25 (3), pp. 213-233.
- Trepte, S. and Reinecke, L. (2013) *The Reciprocal Effects of Social Network Site Use and the Disposition for Self-Disclosure: A Longitudinal Study*, in "Computers in Human Behavior", 29 (3), pp. 1102-1112.
- Tsai, J., Egelmann, S., Cranor, L.F. and Acquisti, A. (2011) *The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study*, in "Journal of Information Systems Research", 22 (2), pp. 254-268.
- Tufekci, Z. (2008) *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, in "Bulletin of Science Technology & Society", 28 (1), pp. 20-36.
- Van der Velden, M. and El Emam, K. (2012) *"Not All my Friends Need to Know": A Qualitative Study of Teenage Patients, Privacy, and Social Media*, in "Journal of the American Medical Information Association", 20, pp. 16-24.
- Viller, S. and Sommerville, I. (2000) *Ethnographically Informed Analysis for Software Engineers*, in "International Journal of Human-Computer Studies", 53

- (1), pp. 169-196.
- Viseu, A., Clement, A., Aspinall, J. (2004) *Situating Privacy Online*, in "Information, Communication and Society", 7 (1), pp. 92-114.
- Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G. and Cranor, L.F. (2011b) "I regretted the minute I pressed share": A qualitative study of regrets on facebook, in "Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11, 10:1-10:16, New York, NY, USA".
- Wang, Y., Leon, P.G., Scott, K., Chen, X., Acquisti, A. and Cranor, L.F. (2013) *Privacy Nudges for Social Media: An Exploratory Facebook Study*, in "Proceedings of the 22nd international conference on World Wide Web companion", pp. 763-770.
- Wang, Y, Norcie, G. and Cranor, L.F. (2011a) *Who is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on social Network Sites*, in "Proceedings of the 4th International Conference on Trust and Trustworthy Computing", pp. 146-153.
- Warren, S.D. and Brandeis, L. (1890) *The Right to Privacy*, in "Harvard Law Review, 4 (5), pp. 193-220.
- Westin, A. (1970) *Privacy and Freedom*, London, The Bodley Head.
- Wisniewski, P. (2011) *Interpersonal Boundary Regulation within Online Social Networks*, in <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05928748>, retrieved September 5, 2013.
- Young, A.L. and Quan-Haase, A. (2009) *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*, in "Proceedings of the 4th International Conference on Communities and Technologies", pp. 265-274.