Article

SM+S
social media + society

Social Media + Society
January-March 2017: 1–14

DOI: 10.1177/2056305117695325
journals.sagepub.com/home/sms
SAGE

Social Media Users' Legal Consciousness About Privacy

Katharine Sarikakis and Lisa Winter

Abstract

This article explores the ways in which the concept of privacy is understood in the context of social media and with regard to users' awareness of privacy policies and laws in the 'Post-Snowden' era. In the light of presumably increased public exposure to privacy debates, generated partly due to the European "Right to be Forgotten" ruling and the Snowden revelations on mass surveillance, this article explores users' meaning-making of privacy as a matter of legal dimension in terms of its violations and threats online and users' ways of negotiating their Internet use, in particular social networking sites. Drawing on the concept of legal consciousness, this article explores through focus group interviews the ways in which social media users negotiate privacy violations and what role their understanding of privacy laws (or lack thereof) might play in their strategies of negotiation. The findings are threefold: first, privacy is understood almost universally as a matter of controlling one's own data, including information disclosure even to friends, and is strongly connected to issues about personal autonomy; second, a form of resignation with respect to control over personal data appears to coexist with a recognized need to protect one's private data, while respondents describe conscious attempts to circumvent systems of monitoring or violation of privacy, and third, despite widespread coverage of privacy legal issues in the press, respondents' concerns about and engagement in "self-protecting" tactics derive largely from being personally affected by violations of law and privacy.

Keywords

online privacy, social media, legal consciousness, awareness, disclosure

Social Media Users and Privacy

Social networking sites (SNSs) continue to grow in popularity. In 2015, the Pew Research Center reported that 90% of young American adults aged 18–29 use social media, compared to 12% in 2005, an increase of 750% (Perrin, 2015). Likewise, in 2013, 89% of Europeans aged 16–24 years were found to participate in social networks (Seybert & Reinecke, 2013). In 2012, the European Commission called for a reform of European Union (EU) data protection rules through which citizens should regain control over their personal data (European Commission, 2015).

In 2010, Mark Zuckerberg, CEO of Facebook, commenting on the rise of SNSs, said that users have become more comfortable sharing their private information online, including challenging the "social norm" of privacy, which, in his eyes, had become obsolete (Zuckerberg quoted by Johnson, 2010).[1] Tracing "Facebook's eroding privacy policy," the Electronic Frontier Foundation (EFF), a nonprofit organization defending rights in the digital world, argued,

> When it started, it was a private space for communication with a group of your choice. Soon, it transformed into a platform where much of your information is public by default. Today, it has become a platform where you have no choice but to make certain information public, and this public information may be shared by Facebook with its partner websites and used to target ads. (Opsahl, 2010)

In thinking about privacy, two emerging phenomena are of particular interest: on the one hand, technological architectures of social media push the boundaries of disclosure—both voluntary and involuntary—accompanied by privacy policy in the terms and conditions (T&C)[2] of use. In response, the question of informed consent has entered European law, to counterbalance a perceived disparity in power between users and social media companies. On the other hand, on the normative, cultural level, debates about privacy today are

University of Vienna, Austria

Corresponding Author:
Katharine Sarikakis, Department of Communication, University of Vienna, Währinger Straße 29, Zi. 7.20, A-1090 Vienna, Austria.
Email: katharine.sarikakis@univie.ac.at

shaped around—and by—the argument that privacy is an obsolete "quest" linked to industry practices that created a business model based on the monetization of the protection of privacy through expensive software.

Users, under a regime of constantly changing private policy are called to negotiate complex technological architectures to determine degrees of privacy in social media. Meanwhile, public law attempts to govern these relations under conditions where the legal concept of "privacy" attains different dimensions in social life. The point at which these two forms of law intersect is arguably situated in the everyday lives of users/citizens. Drawing on the concept of legal consciousness, this article investigates through focus group interviews, the ways in which social media users make sense of privacy as a right and the ways in which they experience and respond to challenges to privacy. Our research aims to explore what role, if any, law—both private and public policy—plays in their lives, by discussing people's (a) understandings of privacy laws and policies (or lack thereof) and (b) the ways in which social understandings of privacy might inform strategies of negotiating the legal dimensions of their privacy (and violation thereof).

The Complexity of Privacy in Scholarship and Law

Although challenges to privacy have lately become more intensive as an issue of public policy in the public debate, interest in exploring conceptions of privacy in policymaking and by the public is not a recent phenomenon. Interest in understanding, defining, and protecting privacy can be traced back to the seminal work "The Right to Privacy" by the Boston law partners Samuel Warren and Louis Brandeis, published in the Harvard Law Review in 1890. Advocating a legal right to privacy, their paper has contributed to and shaped the developments in the treatment, the legal recognition and the protection of privacy in the Western world. The authors raised the aspect of informational privacy and the dimension of unintruded-upon space for thought and recollection.

Scholars have debated the blurry meanings of privacy, often as a problem requiring definitional categorization (Chemerinsky, 2007) and in relation to other individual rights (Solove, 2008). Overall, two concepts of privacy, a *descriptive* and a *normative* conception, can be distinguished. While a descriptive conception of privacy does not include a judgment about, nor an evaluation of, privacy's benefits, a normative conception of privacy anticipates its benefits and value, as well as an entitlement to protection. An early definition of privacy is the limitation of other people's access to an individual in terms of attention, physical proximity, and information (Gavison, 1980). While Nissenbaum (2010) ascribes more importance to characterizations of privacy that define it not in descriptive or normative terms but as a *constraint on access or as a form of control*, legal scholars, such as Gavison (1980), an advocate of *what* is protected as private (descriptive conception), rejects the view that privacy is a form of control but regards control *"only" as part of privacy*. Warren and Brandeis's account is largely of a normative nature, although their concern was predominantly the protection of citizens from mental distress deriving from the publication of their correspondence and personal information, domains considered core for personhood.

In "Transforming Privacy," Scoglio (1998) distinguishes the dimensions of physical, decisional, informational, and formational privacy. Physical privacy relates to the idea that a person enjoys certain protections and immunities in his/her abode and over his/her body. Decisional privacy refers to the decisions and choices of a person with regard to their personal actions. Informational privacy concerns the control a person has over access to information about themselves. Formational privacy, the key dimension of privacy, is characterized by an individual's interest in self-reflection and so-called "critical interiority."[3] Despite differentiated emphasis, "control" over a specific domain of one's life comes into question. There are four categories of legal doctrine that protect individuals from privacy violations: (a) freedom of personal autonomy, (b) the right to control personal information, (c) the right to control property, and (d) the right to control and protect physical space. Mills (2008) points out that the legal recognition of privacy is based on a reasonable expectation of privacy, rather than a personal subjective perception.

However, in practice, *exercising* these privacy dimensions as a matter of citizenship has become increasingly entangled in a trade relation, where privacy is *not a right* but a *commodity*, to be exchanged in return for specific benefits (Campbell & Carlson, 2002). As Papacharissi (2010, s.p.) poignantly notes, "Byte by byte, our personal information is exchanged as currency, to gain digital access to friends." Here, the intervening role of external actors has a regulatory effect, shaping the degree of privacy, in terms of collecting, processing, and disseminating personal information. The State intervenes on the basis that loss of privacy is in exchange for security; market actors capitalize on both the need for human connection online, which produces personal information often in the most intimate form, *and* the need for privacy as compensation for this intrusion.

Legal Consciousness

The complexity of privacy, as raised in scholarship, is found also in legal considerations for public policy. The *absence* of this complexity and the reduction of privacy to an "exchange" through commodification of its aspects is the dominant paradigm in the T&C of social media platforms.[4] The Special Eurobarometer on data protection found that only one-fifth of the respondents are always informed about the conditions of data collection and the further uses of their personal data

when they are asked to provide personal information online. Furthermore, less than a fifth of participants (18%) said that they fully read privacy statements, compared to a third of respondents who said they do not read them at all (European Commission, 2015). T&C constitute forms of private law, which, however, increasingly challenge the protective aspect of privacy as a right, while providing concessions to market logics. Developing legal frameworks increasingly resort to arguments around security and cost efficiency to allow for the collection and monitoring of personal information (Walsh, Parisi, & Passerini, 2015). These two dimensions constitute a battleground where the conflict between public and private interest affects citizens' everyday experiences with and on social media, and the ways in which they accept or challenge the normalization of privacy in its "tradability." Chemerinsky (2007) argues that "any aspect of privacy now suffers guilt by association, making protection of other aspects of privacy far less likely" (p. 651).

The ways in which legal concepts, such as privacy, are socially interpreted and the ways in which citizens deal with them is the subject of the study of legal consciousness. We are interested in the ways in which people negotiate legal dimensions of their privacy (and violation thereof) as social media users, in their everyday life. The process of negotiation is termed "legal consciousness," which connotes a theory and epistemology of aiming to connect law to everyday life. Early studies developed significantly around quantitative questions measuring behavioral changes, by putting "law first." As the field developed, scholars interrogated qualitative dimensions of people's meaning-making of law and the place of law in their lives, even when law is absent. In particular, legal consciousness research aims to explore the ways in which law maintains its institutional power. For Ewick and Silbey (1992), this is to be found in culture, an underexplored terrain. Culture, as a way of life, offers the field where social practices, personal beliefs, and institutional frames meet. Silbey (2005) notes that it is crucial to document the ways in which, and reasons why, the discrepancy between claims of equal treatment to deliver justice and the reality of further generating of inequalities in society persists. For Ewick and Silbey (1992), "[t]he ways in which the law is experienced and understood by ordinary citizens as they choose to invoke the law, to avoid it, or to resist it, is an essential part of the life of the law" (p. 737).[5] Legal consciousness scholarship has drawn on the kinds of formal law that may or may not be paramount in people's attitudes and thinking, and the ways in which it normalizes the existing social relations.

Jacobs (2011), approaching privacy from a legal consciousness perspective, interviewed Canadian youth on their understandings of privacy, privacy rights, and infringements in SNSs and compared those understandings to the policy approach by the Office of the Privacy Commissioner. Jacobs (2011) found that Canadian youth offered a variety of understandings about privacy, but did not know how privacy rights might be, or are being, protected by the law. Yet, according to Jacobs (2011), young people utilize various tactics and provide their own responses to violations of privacy. One of them was "self-regulation." Individualization of responsibility to produce protection and apply legal requirements for one's privacy right may be a meta-reading of this study. Other responses include not to act, or to complain to the social networking platform (in the case of the study, to Facebook).

This article inserts into the discussion the dimension of policy as private law, and situates it adjacent to the existence—or absence—of public law. Increasingly, regulation is privatized through models of self-regulation within industrial sectors as well as on the basis of T&C, in particular in conditions of transnational governance (Büthe & Mattli, 2011; Cohen, 2004; Priest, 1998). Hence, the law is not confined within the "jurisdiction" of the state; in transnational social media platforms, privacy policies of individual companies have gained a hegemonic position in global governance. Privacy law here is arguably weaker in practice. This article orientates itself toward the study of people's meaning-making and interpretation of privacy as a matter of law, as a set of rules applied "equally" on individuals, as a "device," or set of "tools" to govern social relations and as a right—an earned entitlement with the implicit aim to "correct" or prevent social injustice. We explore this process in its connectedness to the ways in which the law as a protective framework, through its presence or absence, is negotiated by people. We focus on social media, in particular SNSs, because of their strong, yet blurred, dichotomy of private/public character. SNS allow and facilitate new forms of socialization, of sharing and communicating online. The vast number of users and the publicness of "their" information pose new challenges to privacy and, thus, social media usage actively shapes and challenges notions of privacy. Even loss of privacy is renegotiated and reframed as transparency and connectedness, underpinning legal dilemmas regarding withholding privacy rights in the fight against terrorism.

Today, research focuses almost exclusively on the degree to which people are aware of the existence of privacy-invading and surveillance technology. Information economics has offered the largest body of literature on perceptions of privacy and users' behavior in the past two decades, exploring the conditions under which individuals understand, that is, conceptualize, privacy and make information-sharing decisions. Such studies are descriptive, "measuring" the economic dimension of privacy in relation to information disclosed. Recent case studies of the usage of SNSs suggest that users overestimate their knowledge and understanding of privacy laws and policies and that this deficit extends to matters linked to technologies, as well as to policies about privacy, trafficking of personal data, and fundamental rights (Acquisti & Grossklags, 2005; Pitkänen & Tuunainen, 2012). Although consumers are fairly familiar with ways to protect their privacy, their use is quite low (Dommeyer & Gross,

2003). Brandimarte, Acquisti, and Loewenstein (2013) suggest, paradoxically, that more control over the publication of their private information decreases individuals' privacy concerns and increases users' willingness to publish sensitive information, even when the probability that strangers will access and use that information stays the same or, in fact, increases. Bechmann (2014, p. 28) speaks of a "non-informed consent culture."

These largely US-based studies mapped out attitudes toward privacy as a matter of disclosing information, before intensified public debate about it as in the case of the "Right to be Forgotten" and the Edward Snowden revelations. The available studies made, at best, rather weak connections to concerns about surveillance, that is, the systematic monitoring by the state of users' information disclosure and non-disclosure. Furthermore, the combination of private corporations' unauthorized or manufactured access to personal data with state-run surveillance over digital communications, creates an environment of intensified threat to the protection of privacy as a human right and as a positive practice. Finally, available studies do not explore or discuss the ways in which legal consciousness on the matter of privacy is developed and articulated on the part of citizens (except for the aforementioned study by Jacobs, 2011). Thus, this article aims to fill these gaps by providing a European perspective and by addressing questions that have not been answered from a US-based perspective.

Method

We gathered data about European social media users' meaning-making, understandings of privacy, and awareness of policies and laws that affect privacy in light of their exposure to salient events of privacy violation. Within the space of 8 weeks, between April and June 2014,[6] the European Court of Human Rights ruled against Google on the basis of the "Right to be Forgotten" and Edward Snowden gave historical testimony to the Council of Europe. Focus group interviews were conducted in the third and fourth week of June 2014.

In order to access diverse viewpoints, we conducted focus group interviews, as they allow for understanding of group processes (Aurini, Heath, & Howells, 2016). Moreover, in focus group discussions, information is elicited in a way that enables researchers to find out not only *why* an issue is salient, but also *what* is important about it (Morgan, 1988). Focus groups were preceded by a short (individual-based) survey on demographic data and basic questions about familiarity with social media sites and services. An interview guide was developed for the discussions on the following themes: the meaning and implications of (online) privacy, control over personal data online (also in the context of the "Right to be Forgotten" and the Snowden revelations), and knowledge of laws that protect personal information (online). Potential focus group participants were recruited via email and flyers, followed by an email to confirm participation and date, time, and location. The focus group discussions were conducted in English,[7] audio-recorded and transcribed ad verbatim for analysis. During the focus group interviews, either the assistant note-taker or the interviewer herself took copious notes on non-verbal behavior (e.g., participant knitted her brows together in concentration; the group was amused by this remark; direct responses to discussants). The transcription took place immediately after each group discussion: thus, data collection and analysis were concurrent. The transcript-based analysis drew on Grounded Theory, specifically on constant comparison analysis (Glaser & Strauss, 1967). Procedurally, we followed Strauss and Corbin's (1990) three major coding stages in Grounded Theory approaches: open coding, axial coding, and selective coding. During the first stage, open coding, the data were broken down into small units, examined, compared, conceptualized, and categorized. During the second phase, axial coding, the fractured data were put back together in new ways by making connections between the categories and subcategories. Finally, in the third phase, selective coding, the researcher develops or selects a core theme and relates it to other themes (Strauss & Corbin, 1990, p. 116). Through constant comparison analysis, we assessed general and across-group saturation, important in particular for focus group research with multiple focus groups (Onwuegbuzie, Dickinson, Leech, & Zoran, 2009).

We ran seven focus group interviews of female and male Vienna-based[8] students,[9] enrolled in Natural Sciences and Social Sciences programs, without prior studies in privacy or privacy law. A total of 44 students took part; the average focus group lasted approximately 52 min (range 36–68 min). As highlighted by Stewart and Shamdasani (1990, p. 94), the moderator has to gage the extent to which a topic or issue had been exhausted. When further discussion was believed unlikely to yield substantive new information, and the pace of the focus group allowed, the moderator moved on to the next question. Participants' mean age was 28 years (SD = 5.6, range 21–45). The characteristics of the groups compare well to what we know about social media use in the EU. Out of 44 participants, 87% stated that they had Internet access on their mobile phones, compared to 13% who did not. Facebook and Twitter were the two SNSs that every participant had at least heard of (see Figure 1).

In comparison, in 2013, 44% of Europeans used social networks at least once a week, according to a survey (European Commission, 2013). Table 1 elaborates on participants' Facebook and Twitter use in detail.

Privacy as Personal Autonomy and Control

Most subjects' perceptions of privacy evolve around the idea of personal information and private space. Privacy attains predominantly a meaning of protected "space," not only in

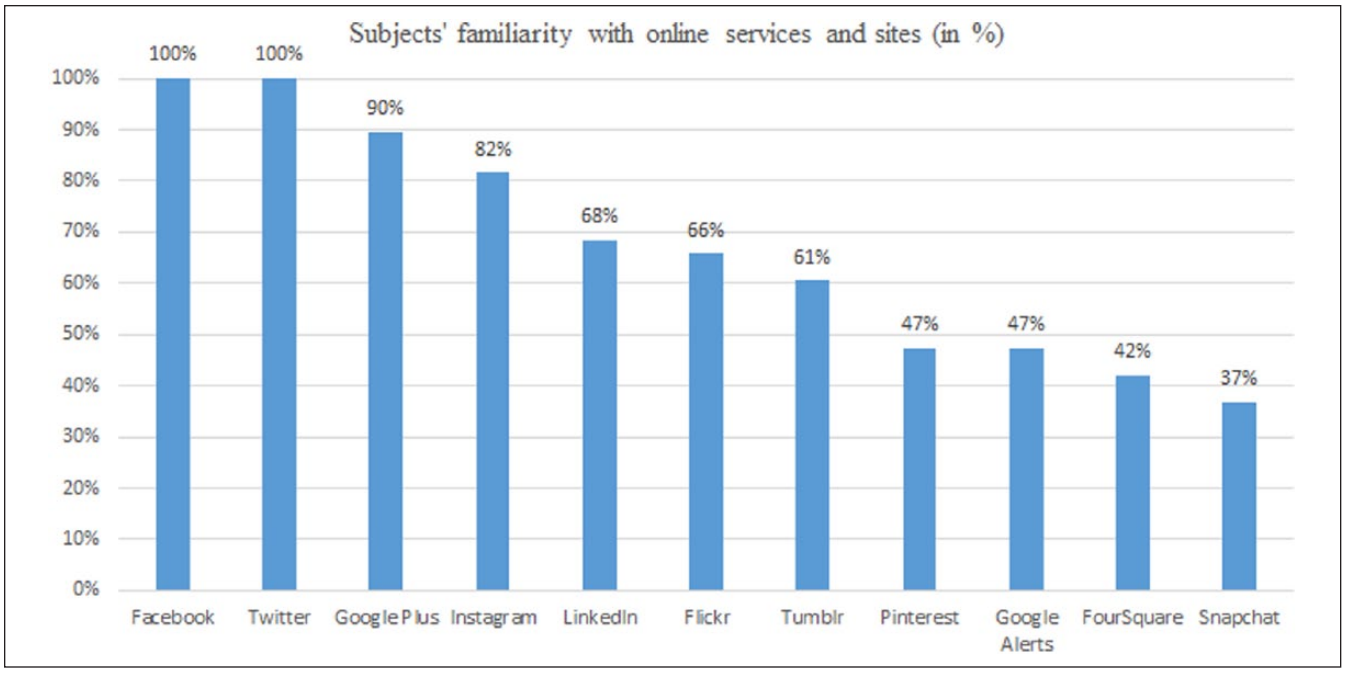

Figure 1. Subject's familiarity with online services and sites (in %).

Table 1. Subject's Facebook and Twitter use (in %).

	Subject's Facebook use	Subject's Twitter use
No, have never used it	5	38
Tried it once, but have not used it since	5	24
Yes, have used it in the past, but do not use it nowadays	5	16
Yes, currently use it sometimes	16	11
Yes, currently use it often	69	11
	100	100

terms of "simple" personal data but also in terms of social interaction and the kinds of information these generate:

> For me privacy is something that really involves just me and [. . .] nothing else. (Female, 23)

> It's my personal space when I can decide for myself who has access to this and who not [sic]. (Female, 29)

With regard to the question, "What does privacy mean to you?," the conversation oscillated between negative—others are not to have access to your information—and positive—to have control over what you want others to know—definitions. In all groups, the discussions quickly turned to the connection to "real life," underlining the continuum of online and offline privacy. A common thread in the discussions was the idea that one's privacy is determined by the capacity or not to control the publicness of their information. Even if this publicness might be a broad one, the qualifying difference is the ability and capacity to withdraw, restrict, limit, and deny access to this information. This is understood to be a process taking place at any given time, without any predetermined conditions of who or what might access information generated by the subjects—be it data or feelings, bookmarks and "likes." The only constant factor against which privacy is "measured" in these discussions is "others": others than those to whom the subjects want to disclose information. Tellingly, respondents' approaches linked elements of personal data with spaces protected from forms of intrusion from the outside world and were directly connected to a sense of "law" and legality around the protection of their data and "spaces":

> [Privacy] means that I can decide who is going to see what I am doing but it is not possible on the internet [. . .]. (Female, 23)

> [Privacy is] I can be sure that not everybody can read what I write on my [Facebook] wall but when it comes to Google, privacy means to me that I am not sure because Google saves [searches]. (Female, 28)

> If there is something that I don't want people to know, so that's my privacy [. . .]. (Male, 33)

Thus, subjects' approaches placed the self at the center of privacy—always as the legitimate "controller" of privacy—even when in cases in which fatalist comments on the futility of expecting privacy in the digital world are made. This understanding is connected to an undisputable sense of "ownership" over personal data, for instance, subjects' date of birth, even if such information might be accessible through other, institutionalized ways, and over information, that concerns one's identity. In fact, for respondents, privacy is linked closely to the right to privacy. The majority of the subjects considered the right to privacy to be a means to protect the kind of information they view as private:

> Personal relationships, for example every time when I am on Facebook it says that your profile is only 1% complete [. . .] I don't want to share this personal stuff. (Female, 25)

> [. . .] personal relationships with people, family, things like that, everything else I am not involved enough, they can have it if they want, if they care. (Male, 30)

The quotes above show that personal data or personal information were used indistinguishably to refer not only to what the law regards as such (e.g., date of birth, national security number) but also as an expression of opinions, as well as of emotions, and associations with people or causes. When asked what things they believed the "web" knew about them, the answers commonly ranged from "everything" and "too much" to "a lot." *No respondent offered a different view*. When asked to describe in detail, they spoke as if reciting, one after the other, or sometimes one talking over the other:

> For example your name, your date of birth, your address or what you like, what you dislike, who are your friends, for example, if you are sick or you feel sick and if you google on the internet what it could be. (Female, 24)

> My location, where I am now, when I am travelling, my work, my studies. (Female, 27)

> I think they know a lot. Where I am [sic] born, what I did in my BA or Master's study [. . .] or where I was on holiday, where, how many times [. . .]. (Female, 37)

> [. . .] I think with mobile phoning and the internet knows every step of you. (Male, 27)

The potential impact of a tracked life online that leaves unerasable traces is something that participants find scary:

> They have like people started to document [sic] their life of their children. In the end they can do such a video with all the pictures appearing, which appear on Facebook, a video of your personal life. This was like a scary thought for me. (Female, 25)

The "individual" stands at the core of a continuum between control over information and loss of privacy. Additionally, the implied disempowerment through a life fully monitored without one's own knowledge or agreement offers an unnerving image.

So, privacy for the respondents was not only about the "what" (i.e., what kind of personal information), but also about the "who" (i.e., who has access to their personal data). In fact, a common understanding of the right to privacy was the control over who may have access to personal data:

> I am sure that it is more people than I think. (Male, 28)

> [. . .] I am not so comfortable anymore about getting linked on photos on Facebook or posting things that contain personal information [. . .] I don't want people who don't know me, to know. (Male, 29)

When asked how much control they (think they) have over their personal data online, respondents reported feeling under surveillance and "being watched" coupled with a paradoxical sense of fatality and acceptance, for some even resignation (there is little control over one's personal data and little one can do):

> I wouldn't connect privacy with the web, because I have got the feeling that [. . .] if you are online, there is always someone else who can see what you are doing. (Female, 23)

In the groups, references to inevitability recurred throughout the discussions at several stages. They were met sometimes with a sense of resignation and often with anger by the respondents directed at this inevitability but also as a reaction to the widespread feeling of helplessness:

> It can't be controlled [. . .] if you're putting something [online] then you know it will end up somewhere [. . .] I think you need to work on minimizing the chances and I think it can't be controlled. (Male, 33)

> I can just say that I don't know how much privacy I have when I am surfing the internet. (Female, 31)

A survey on citizen's behaviors and attitudes concerning identity management, data protection and privacy in 2011 by the EU showed that only a small percentage of social networking users (26%) and even fewer online shoppers (18%) felt in complete control in Europe (European Commission, 2011). In Austria, even fewer users (17%) felt they had complete control over the information they have disclosed on SNSs and/or sharing sites. More than 60% of Austrian users felt they had partial control and one-fifth felt they had no control at all (European Commission, 2010). In 2015, fewer people, 15%, felt they had the ability to correct, change, or delete this

information. More than 8 out of 10 participants reported that they did not have complete control over their personal information; two-thirds were concerned about not having complete control over their information online (European Commission, 2015).

In our focus group interviews, people were categorical—and spontaneous—about the degree of control they had over third-parties (e.g., companies) accessing and monitoring their web behavior:

> None. (Female, 37)
>
> Very little. (Female, 27)
>
> I think it should be a little [control]. [. . .] I don't really trust Facebook or any other social media as if they want somehow to share this information [. . .] and maybe it's useful information for them. (Female, 37)
>
> When you think of Facebook, for example, you can indeed customize what users see [. . .] and yet what is displayed on Facebook and what really reaches my friends is a completely different story and the collection of data of Facebook the company itself is without [sic beyond] my control [. . .]. (Female, 38)

Overall, 58% of respondents of this study believed that even when a web site had a privacy policy, it would share their information with other sites or companies. Furthermore, 74% out of 42 respondents believed that web sites were not required to indicate to them if they were tracking their online behavior and even more participants (84%) believed that when they went to a site, the site could collect information about them even if they were not registered on it. Almost all respondents (97%) were under the impression that today's companies had the ability to place an online advertisement that targeted users based on information collected on users' web browsing behavior.

This "data insecurity" echoes studies, which suggest that adults have little confidence that their records, from government agencies to credit card companies or social media sites, would remain private and secure, despite the existence of laws protecting personal data. In a 2014 survey on "Americans' Attitudes about Privacy, Security and Surveillance" by the Pew Research Centre, for instance, 45% of the participants had little confidence that the social media sites they used would maintain their data private and secure (Madden & Rainie, 2015). Turow, Draper, and Hennessy (2015, p. 4) found that "a large pool of Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data." In addition, their survey indicated that more than half of the interviewed Americans *does not want to lose control* over their personal information, but at the same time believes that this *loss of control has already happened*. Thus, they feel "a lack of autonomy" (Turow et al., 2015, p. 4).

Negotiating Privacy: Self-Silencing, Self-Regulating, Resignation

A form of resignation with regard to control over personal data appears to coexist with a recognized need to protect one's private data. In each group, we found that there was a small minority, usually of one vocal member, who seemed to accept the loss of privacy as something to be expected—even normal—something that one could not do anything about and: "Why should they?" It is this interesting exhibition of defiance which can be read as an attempt to regain control by repositioning oneself in the relationship of user and company (or State) in "knowing it all about you" and in refuting the possibility of harm or ethical wrongness about this.

In several discussions, group members "naturally" included Google and email to talk about social media, showing interconnection and also emphasizing what they viewed as "normal," although suspicious and unwelcoming:

> The cookies and [the fact that] other pages can see what you have done and [. . .] Google sees your profile although you are not registered with Google, they know your mail or emails or they guess your email, and they have your demographic information and what else, what else, what else and yeah [. . .] although you are not registered on the page they know you. So that is definitely not privacy [laughter]. (Female, 28)

Upon the last remark, the other group members started to laugh wryly, and the aforementioned 28-year-old subject joined in.

The dimension of technological literacy as a method of maintaining control and negotiating the ever-changing policy default landscapes of social media prompted lengthy discussions. Technological capacity, through advanced knowledge, was considered possibly the most important factor in the struggle to maintain privacy and control over private information by the focus group participants. Various tactics were discussed, such as use of alternative non-intrusive media, fake profiles, advanced manipulation of settings, and so on. The discussions showed that young people were knowledgeable about at least the role of in-depth technological expertise and could distinguish it from surface skills in using technology and accessing platforms, echoing Jacobs's (2011) findings. Few explained in detail how manipulation of technological resources might provide some source of protection but everyone agreed that this was a skill that demanded time and other resources.

The regulatory effect of technology in general—and the technological capacity of the user as a tool to circumvent intrusive social media tactics in particular—became clear in the discussion. Those respondents who were (or felt) confident with technology considered themselves to be in control of what they did and did not share with others. Hence felt *empowered and autonomous*. They listed an array of tactics they deployed to (re-)gain control, their response being met

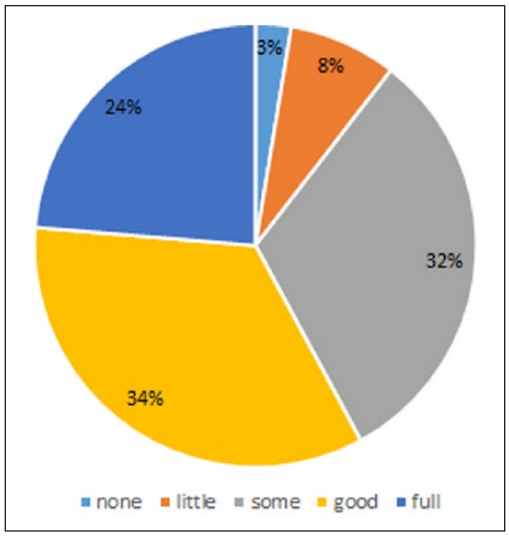

Figure 2. Participants' claimed understanding of privacy settings.

with reactions of admiration for their skills by fellow members of the group:

> Quite a lot of possibilities to do this [protect privacy] but you must have the knowledge about it. So [. . .] you can change your IP address, you can change your whole data transfer, you can change other servers [. . .] you have possibilities but you must have a lot of knowledge [. . .] and it's a lot of energy and a lot of time you need to invest to protect your privacy on the internet [. . .]. (Male, 27)

Our short survey suggested that participants rated their understanding of privacy settings higher in the standardized questionnaire than when they were actually asked about it in person. For example, 34% and 32% of respondents, respectively, stated that they have good or some understanding of privacy settings, compared to only one-fourth of respondents who said that they have full understanding of privacy settings (see Figure 2).

These figures are, at first sight, *in stark contrast* to Butler's, McCann's, and Thomas's (2011) study on users' awareness of privacy settings on Facebook. They found that only 14% of their respondents had read the latest version of Facebook's privacy policy compared to 17% who had only read the privacy policy when they first set up their account, and 21% said that they had only read parts of it, while the majority in Butler's, McCann's and Thomas's survey (41%) admitted that they were either partially or completely unfamiliar with Facebook's current privacy policy. Moreover, 82% of respondents said their postings were only visible to people in their friends list.

Likewise, during the focus group interviews of this study, respondents commonly admitted that they had little or no understanding of privacy settings:

> I don't know about this technical stuff, I didn't know it existed so I can't do this, but for instance when you start doing your privacy settings on Facebook it's really very very complex [. . .] I think there are various things you can do but you have to be aware of it and you have to do the work and you have to be really really willing to do it. (Female, 25)

The comment was followed by break-up discussions that ran parallel to the difficulty of keeping abreast with technology in this race. The discussions moved across three positions: resignation and acceptance found in one person in each group, self-regulation adopted by the majority (restricting oneself), and specialized technical counteraction, typically seen in one or two members in each group:

> I also don't have the technical knowledge to do all this [. . .] so the easy way is not to be so much on the internet or just on these sites you trust and [. . .] go to shops and meet friends, not internet friends, in real life friends [. . .]. (Female, 31)

Self-regulation appears to be one of the dominant tactics to negotiate privacy especially given that most respondents declared being unsure as to the policies and technological capacities and actions of social media. Trottier and Lyon (2011) argue that social media continuously adopt new features and that users have difficulties to understand these updates. Privacy settings depend on the architecture[10] offered by the platform and are governed ultimately by the T&C. The issue of keeping up with Facebook in particular and its constant changing of the "rules of the game" is an integral part of the respondents' attempts to regain control. The struggle is ongoing and evolves, requiring vigilance on the part of the user and alertness to changes employed by Facebook. Some make references to a "lost game" in part: either realizing the possibility to react too late, by which time Facebook had disabled opt-out choices, or the notion that configurations cannot be affected by users. Just under 60% of the respondents declared a lack of knowledge of the concept of limited profile (34% had no and 26% had little understanding). Yet, respondents reported fatigue, distrust, and uncertainty as users of the platform:

> I tried but somehow they [Facebook] change the system all the time and it is very difficult to follow that [. . .] sometimes I delete some pictures but I don't know if it is really deleted from the system [. . .] and I just won't see it. (Female, 37)

> I am more paying attention to what I am posting on Facebook and how I post it. [. . .] one year ago I just post[ed] everything and I did not really check who can see it and now I realized that often I actually post something for everybody, which scared me a bit because I just did not see this little option that you change to only friends, public and so on. (Female, 27)

One participant replied as follows to the suggestion that individual responsibility might also be important in determining what becomes public on social media:

> [. . .] I think it is just really difficult. Even if I wanted to, I think it's also because you are just not educated enough to understand what actually they are telling you in the conditions. So my biggest problem is that I don't have the patience to read it through and I don't even know how to understand it sometimes and I am not sure if I can imagine [inaudible] because there are always implications and I am just not able to interpret in the right way. (Female, 27)

Another 27-year-old female subject continued this thought and briefly referred to some strategies she uses to regain control over her privacy:

> Yeah, the privacy policy is really quite complex and long and maybe if you really think about it. But I never posted that much [sic] personal things on Facebook and for me it is also important to delete cookies, the cache and also to do privacy settings on my browser not just on the social media sites, also on your browser so. (Female, 27)

At the same time, privacy appeared to be linked to the ability to also provide false information about oneself. Respondents reported using fake names on the Internet, especially when it came to Facebook, in order to protect their privacy:

> I never use my actual name on Facebook. (Female, 38)

> I stopped using my real name on Facebook and right now I am using my fake account, because [. . .] I think I had to do it. (Male, 32)

> I also changed my private name on Facebook. (Male, 27)

> Well when I use fake names or email addresses and fake birthdates I think that's the only control you can try to have. (Female, 28)

At the time the focus group interviews were conducted, subjects using fake names actually violated Facebook's policy of requiring use of birth names on accounts. In response to activist groups among others EFF, Human Rights Watch, and American Civil Liberties Union (ACLU), Facebook recently issued a statement revealing changes to its real names policy. On that note, Facebook also emphasized that it would remain "firmly committed" to this policy: "On Facebook, we require people to use the name their friends and family know them by" (Osofsky & Gage, 2015). EFF dismissed the introduced adjustments as "rearranging chairs on the Titanic" (Ben Hassine & Galperin, 2015).

Familiarity With and Expectations From the Law

Despite widespread coverage of privacy legal issues in the press, respondents' concerns about, and engagement in, "self-protecting" tactics derived largely from being personally affected by violations of law and privacy. In one of the focus groups, a participant raised the issue that the discussion only centered around users as subjects and that it did not pay attention to the Internet and its architecture itself:

> I think that I also understand privacy from the point of the internet, from the rules and terms that they are using for . . . privacy, for me, for each of us. (Female, 32)

Two other participants of that particular focus group nodded in agreement with this statement, while another member shrugged his shoulders. In general, most subjects showed that they may be aware of privacy risks, but that they had a limited and fuzzy knowledge about how and/or where and by whom their right to privacy was protected:

> I also don't know the laws by names but I know that there are even many directives also coming from the European Union and I know one law from Poland to protect privacy. (Female, 29)

> I know there is the Datenschutzgesetz in Austria but I don't know how it works. (Male, 28)

> In the UK there is this data protection law [. . .] I just well [laughter] if you wanna buy something or so. (Male, 31)

Likewise, in 2011, only one-third of Europeans (33%) were reported to be aware of the existence of a national public authority responsible for protecting their rights regarding their personal data (Eurobarometer, 2011). In all focus groups, not a single respondent was able to refer correctly to a policy or law, or to principles, protecting the right to privacy on a national- or European-level. Instead, some respondents tended to trivialize and relativize the extent and duration of private information available online, as a tactic to neutralize the risk of their rights becoming personally violated. There was also conflation between privacy laws online and cybercrime laws addressing, for example, fraud. The responses showed confusion and lack of knowledge, as well as lack of confidence in respondents' own information:

> I am not really interested. I think at the same time there are so many users, so many [sic] private information and I think it's no so [sic] big deal, my private information. (Female, 37)

> You have data protection laws that regulate how companies spread your data out, that's what is written in the blurb at the bottom isn't it? (Male, 28)

> I think the most commonly used right in Austria that you have is that each website has to put the [its] privacy policy on the website that you can read which information they are collecting and what they are using it for. (Female, 28)

> Some from the European Union and it's about who saves your online banking data that they have an agreement that the banks couldn't give the user data the gratification on outgoing companies or something like this? (Male, 27)

This is interesting insofar as the focus groups were conducted about 3 months after the Court of Justice of the European Union had acknowledged that under EU Directive 95/46/EC, EU citizens had the right to request the Internet search engines such as Google to remove search results directly related to them (Court of Justice of the European Union, 2014). Strikingly, 58% of respondents answered in the questionnaire that if you asked a search engine to remove a search result about you, the search engine was required to remove it. During the focus group discussions, however, it appeared that the majority of interviewed subjects were not entirely familiar with "Right to be Forgotten" but had just heard or read about it somewhere without taking any further interest. Those subjects who were familiar with the "Right to be Forgotten," were doubtful about its efficiency.

A 28-year-old female student claimed, "It should be possible that you can delete all your stuff on the internet." Another woman, aged 23, hastily added, "[I]t's all the stuff." The 28-year-old seemed to feel vindicated and continued, "Yeah, personal things." A 25-year-old female student knitted her brows together in concentration and admitted that she could recall the context in which she had heard of the "Right to be Forgotten," but assumed that "[. . .] it is this right to be erased on the internet":

> I don't know about, but yes, I agree [laughter]. (Female, 32)

The 28-year-old woman said flatly "You can, for example, write to Google that they should, yeah, that they should not list some information of you, but only in special cases":

> I guess it is something with Google [. . .] there was a court case about one guy who had some old data in the internet and said to Google that he wants that this data can't be searched and he won the case. (Male, 28)

To which this female responded,

> But the problem is that there are some websites linked to other websites [. . .] if you are searching another engine you can find [it]. (Female, 26)

> There are also some websites like Backmachine.com [refers to the Internet Archive "wayback" machine], you can google there or search there some websites from 10 years ago that aren't any more on the internet and you see the full homepage in front of you. (Male, 22)

More respondents, not all, had heard of Edward Snowden than of the "Right to be Forgotten." Yet, the majority of respondents said that they had not changed their Internet behavior due to the National Security Agency (NSA) revelations. The Pew Research Center, likewise, found that the great majority of respondents (91%) had not made any changes with regard to their online or mobile phone use to avoid tracking of their activities (Madden & Rainie, 2015).

In response to the question about what, if anything, the world might have learned from the revelations by whistleblowers Julian Assange and Edward Snowden, most of the participants expressed feelings of vindication with respect to their belief that they did not have privacy online (see above) and that even their "offline" privacy, in the sense of their phone call history and their text messages, was threatened:

> We all know it, but maybe it is better to imagine that it is not happening, because everybody knew it and then when they started saying about that they are recording conversations. (Female, 26)

Focus Group Discussions Revisited

We commenced this project with the aim of asking specifically whether knowledge about mass surveillance is reflected upon by young, highly educated, and technologically privileged users in their everyday social media practice, and, by drawing on the concept of legal consciousness, whether and how the legal and regulatory frameworks are interpreted, experienced, negotiated, or reinforced. We realized that expected and unexpected approaches coexist in a complex context of negotiating knowledge about, everyday experience with, moral expectation from and confrontation with privacy as a right. In other words, the legal consciousness of a highly privileged social group is built upon and through both first-hand experience and degrees of knowledge accompanied by degrees of skills and confidence in shaping one's own technological universe. We see that formal knowledge of the privacy laws is subsumed to strong approaches to privacy as a legal right and entitlement. Importantly, there is a strong *common* understanding about the consequences of governing privacy through private law, that is, T&C irrespective of the degree of technical knowledge or understanding of T&C in detail. These findings are, we argue, important, and must be seen against the context of further meaning-making factors active in people's lives.

For a start, in the minds of this group at least, social media are not distinguished in any significant manner vis-a-vis all online platforms and services, in terms of privacy: respondents spoke interchangeably about social media (Facebook and Twitter), Google, email, connection apps, and mobile technologies, highlighting unintentionally that the analytical distinctions we make have little relevance in their lives, when it comes to the question of whether one can—and to what extent—protect one's privacy.

This study found that users' understandings of privacy incorporate both mutually supporting descriptive and normative dimensions, centered predominantly around the notion of *control and constraint* of access to information one deems personal, echoing both the works by Gavison (1980) and Nissenbaum (2010). In the "Post-Snowden" era, however, users' concept of privacy is a negative concept, informed by their *lack of confidence and trust* that social media

companies and third-parties will *keep their personal data private and secure and that the state will protect their rights.* However, they also demonstrate *a sophisticated definitional approach to privacy* built around a sense of *autonomy* (physical, informational, decisional) and control over degrees of publicness of critical interiority. We found more sophisticated analyses, coupled with strong normative positions, are largely represented by those respondents who are aware of the Snowden case, and who keep themselves informed about T&C changes. These are also the people with the highest technological skills, based on autodidactic processes of acquiring them. Interestingly, although no participant withdrew completely from social media, several reported changes in their behaviors, which ranged from posting less, posting differently, and engaging in active ways of protecting their privacy after the "Right to be Forgotten" ruling and the Edward Snowden revelations. Those who stated continued their use as before, were, overall, the minority. Respondents not only determined who had access to their personal information (e.g., via the settings of social media sites), but also *questioned their engagement in SNSs* per se.

Instead of relying on and/or informing themselves about existing privacy policies and laws, their enforcement or lack thereof, the participants' negotiating strategy was rather to restrict themselves, emphasizing what Scoglio (1998) called the decisional dimension of privacy, as an ultimate measure possibly of exercising agency in a situation where feelings of immobilization and deprivation of choice prevail. Even though respondents rarely reported reading T&C of social media platforms, it appears that they had internalized the reduction of privacy to a matter of "exchange" and its commodification. Although focus group participants had a clear and common understanding of what kind of personal data was private, participants, ultimately, seemed unaware of how legal frameworks (might) affect their daily lives, largely because of the sense of law as something distant and non-activatable, and unable to protect their rights. Instead, respondents showed confusion and lack of precise knowledge when it came to negotiating legal dimensions of their privacy and violation thereof, although they did have a good grasp of what was at stake and the dimensions of privacy violation in general. Users' process of negotiation was not based on accurate or deep understanding of either formal privacy law (EU or national) or private T&C policies of the platforms they were using. Yet, to claim legal illiteracy in these areas would be unfair, as it would deny them recognition of a moral understanding of privacy that surpasses formal or other modalities of policy. With regard to our discussions, the majority of respondents were somewhat familiar with the "Right to be Forgotten" and with the NSA revelations and the privacy risks involved, but as symptoms of a larger regime of privacy violation. Although EU legal frameworks on data protection are more rigid compared to US legal sources of data protection legislation, the resignation of EU citizens seems to echo the findings of US studies.

Legal consciousness therefore in this case consolidates a diet of practices that have as their negotiating focus the process of self-discipline and a turn to the self with little orientation to a social or group-based response. We did not find enough evidence of a more socially engaged and oriented legal consciousness among respondents who would, for example, take the form of social movement or other coordinated action. This does not mean that there is absence of such negotiating and meaning making processes, but rather that more research is needed to unearth such processes. Nevertheless, even at the level of—rather—individualized negotiation, it is clear that it is through processes of social sharing of practices that knowledge about tactics and strategies is spread.

Although Mills (2008) argues that the legal recognition of privacy is not based on a personal, subjective perception, participants attempt to regain lost autonomy through: acceptance—or resignation—in exchange for services; technological guerilla tactics of diversion, "camouflage" and manipulation; and self-regulation over expression and connection. Participants all agreed on their loss of control and that even technological counteraction was resource-intensive and unattainable for the majority. The regulatory effect of technology in general—and the technological capacity of the user as a tool to circumvent intrusive social media tactics in particular—became clear in the discussion, raising the discussions' tone and intensity with heated arguments and laughter. The groups always engaged in an emotional debate about privacy: there was always a minority who argued that "internet comes with it" (loss of privacy) and that critiquing this was nothing more than "moaning." These views clashed with those of the most technologically skilled participants, but were also reacted to by more moderate members. We saw indications of an ideological battle being played out among these positions, which expressed not simply personal feelings, but importantly perhaps political dispositions that we suspect concerned further dimensions of the role of the Internet in modern societies, possibly predominantly as free space of expression or a commercial space. The findings of this study show that technological expertise, and hence, other skills and resources upon which the acquisition of advanced technological knowledge might depend, are relevant to the development of tactics on behalf of individual users to (at least temporarily) counterbalance the strategic management of information retrieval and data mining of social media sites. The lack of specific knowledge about existing privacy legal provisions does not necessarily mean that the answer to empowerment of users lies in attaining more information. Not only is this problematic, as theoretically information is generally "available" about T&C and legal instruments, but also because especially in the case of T&C, frequent changes are part of the normalization of the privatization of privacy law. This is rather a futile game, where users cannot "win" unless technological or such systems are developed to alert them. Even in this case, the options left for users remain the

same: self-censorship and self-regulation, more technical skills for the few, withdrawal. Privacy policy options then would have to move beyond the format of informed consent, that is, the individualization of privacy, but would rather aim to regulate the range of processes of data exploitation companies would be allowed to pursue. From monitoring mechanisms and self-regulatory industrial auditing to oversight by independent authorities, these are some of the systems—focused potential policy responses as a matter of global coordination. We are aware that these are complex and hard-to-achieve goals.

Taking these findings and current literature on the subject into account, future research should study trace data and examine other factors, such as sensitivity of disclosed information as well as age, to investigate understandings, expectations, and negotiation processes by users. Since this study used a convenience sample, all participants had a university background. It would be useful to explore groups with a different (at least educational) background. Women, who have been found to be more active on social media sites, specifically raised concerns about being targeted by online advertisers and their lack of technological confidence, to protect their privacy. This seems to be another field in need of elaborate systematic investigation.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The research was funded by the University of Vienna.

Notes

1. Since then, Zuckerberg has assured users that their privacy concerns have been and will be taken seriously—new features were minimally adapted (e.g., News Feed) to please the public, and "user control" and/or "user options" were highlighted (Goel, 2014; Zimmer, 2014).
2. Terms and Conditions (T&C) detail special and general arrangements (rules) of a contract. Users/Contracting parties must agree to the T&C in order to use a service (i.e., social media).
3. Scoglio (1998, p. 233; original emphasis omitted) argues that the powerless actively engage "[. . .] in promoting the inner rise to power of our lower (consumeristic, wealth-maximizing) selves [. . .] and the fantasizing self that lives in TV and media dreamland."
4. Legal frameworks on privacy are not homogeneous across countries, and it is beyond the scope of this article to discuss jurisprudence and law differentiations. However, despite differences, in Western societies legal frameworks on privacy are underpinned by a moral commitment to privacy as a human right.
5. The empirical study of legal consciousness has been questioned, for instance, by Levine and Mellema (2001) and Garcia-Villegas (2003). With reference to Silbey (2005), Hertogh (2009) summarizes their original research agenda along the following three aspects: (a) more emphasis on the role of law in society, (b) more emphasis on the role of ordinary citizens, and (c) a shift in focus from measurable behavior to meanings and interpretations.
6. An April 2014 Google search showed: over 300,000 entries for Edward Snowden, 20,000 of them news-related; 150000 entries for the "Right to be Forgotten," and over 120,000 of them in the "news."
7. All focus group interviews were conducted in English so that non Austrian students could also take part to better reflect the student body. At times participants used German words and phrases—these instances have been translated by the author and marked as translated phrases in the transcription.
8. Vienna is a so-called Smart City and was rated one of the *Top 10 Internet Citie*s in 2013 (criteria such as connection speed, WiFi availability, security, and data privacy were taken into account) (Wien.gv, s.a.). Austria ranks 12th out of the 28 EU Member States in the Digital Economy and Society Index 2016 (DESI). The country's overall score of .56 is above the EU average and Austria is reported to have developed faster than in the EU over the past year. DESI is a composite index developed by the European Commission to track the development of EU countries toward a digital economy and society (DESI, 2016).
9. Half of the participants were white Austrians, one-third white other Europeans, and 19% were Asians, corresponding well to the multi-ethnic context of the University of Vienna.
10. See also Lessig's (1999) modalities of regulation in "Codes and Other Laws of Cyberspace", where he describes code and technological architecture as one modality of law, next to law itself, social norms, and markets.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*, 24–30.

Aurini, J. D., Heath, M., & Howells, S. (2016). *The how to of qualitative research*. London, England: SAGE.

Beckwith, R. (2003). Designing for ubiquity: The perception of privacy. *IEEE Pervasive Computing*, *2*, 40–46.

Ben Hassine, W., & Galperin, E. (2015). *Changes to Facebook's "real names" policy still don't fix the problem*. Retrieved from https://www.eff.org/de/deeplinks/2015/12/changes-facebooks-real-names-policy-still-dont-fix-problem

Bechmann, A. (2014). Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies*, *11*(1), 21–38. doi: 10.1080/16522354.2014.11073574

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*, 340–347. doi:10.1177/1948550612455931

Butler, E., McCann, E., & Thomas, J. (2011). Privacy setting awareness on Facebook and its effect on user-posted content. *Human Communications*, *14*, 39–55.

Büthe, T., & Mattli, W. (2011). *The new global rulers: The privatization of regulation in the world economy*. Princeton, NJ: Princeton University Press.

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*, 586–606.

Chemerinsky, E. (2007). Rediscovering Brandeis's right to privacy. *Brandeis Law Journal*, *45*, 643–657.

Cohen, D. (2004). The role of the state in a privatized regulatory environment. In K. Webb (ed.). *Voluntary codes: Private governance, the public interest and innovation* (pp. 35–56). Ottawa: Carleton Research Unit for Innovation, Science and Environment.

Court of Justice of the European Union. (2014, May 13). *Judgment in Case C-131/12* (Press Release No. 70/14). Luxembourg. Retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

Digital Economy and Society Index. (2016). *Digital Economy and Society Index 2016*. Austria. Retrieved from https://ec.europa.eu/digital-single-market/en/scoreboard/austriahttps://ec.europa.eu/digital-single-market/en/scoreboard/austria

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*, 34–51. doi:10.1002/dir.10053

European Commission. (2010). *Eurobarometer 74.3: Attitudes on data protection and electronic identity in the European Union* (Country report). Austria. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_at_en.pdf

European Commission. (2011). *Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union*. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Commission. (2013). *Eurobarometer 80: Media use in the European Union* (Report). Retrieved from http://ec.europa.eu/public_opinion/archives/eb/eb80/eb80_media_en.pdf

European Commission. (2015). *Special Eurobarometer 431: Data protection* (Report). Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Ewick, P., & Silbey, S. S. (1992). Conformity, contestation, and resistance: An account of legal consciousness. *New England Law Review*, *26*, 731–749.

Garcia-Villegas, M. (2003). Symbolic Power Without Violence? Critical Comments on Legal Consciousness Studies. *International Journal for the Semiotics of Law*, *16*, 363–393. doi: 10.1023/B:SELA.0000013846.61056.a3

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*, 421–471. Retrieved from http://www.jstor.org/stable/795891

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, IL: Aldine.

Goel, V. (2014, May 22). Some privacy, please? Facebook, under pressure, gets the message. *The New York Times*. Retrieved from http://www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html?_r=0

Hertogh, M. (2009). What's in a handshake? Legal equality and legal consciousness in the Netherlands. *Social & Legal Studies*, *18*, 221–239. doi:10.1177/0964663909104191

Jacobs, L. (2011). *Privacy rights mobilization among marginal groups in Canada: Fulfilling the mandate of PIPEDA*. Retrieved from http://ycppl.info.yorku.ca/files/2013/05/Privacy-Rights-PIPEDA-paper.pdf

Johnson, B. (2010, January 11). Privacy no longer a social norm, says Facebook founder. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Levine, K., & Mellema, V. (2001). Strategizing the Street: How Law Matters in the Lives of Women in the Street-level Drug Economy'. *Law & Social Inquiry*, *26*, 169–207. doi: 10.1111/j.1747-4469.2001.tb00175.x

Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance*. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mills, J. (2008). *The lost right*. Oxford, UK: Oxford University Press.

Morgan, D. L. (1988). *Focus groups as qualitative research*. London, England: SAGE.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Onwuegbuzie, A. J., Dickinson, W. B., Leech, N. L., & Zoran, A. G. (2009). Toward more rigor in focus group research: A new framework for collecting and analyzing focus group data. *International Journal of Qualitative Methods*, *8*, 1–21.

Opsahl, K. (2010, April 28). *Facebook's eroding privacy policy: A timeline*. Retrieved from https://www.eff.org/deeplinks/2010/04/facebook-timeline

Osofsky, J., & Gage, T. (2015, December 15). *Community support FYI: Improving the names process on Facebook*. Retrieved from http://newsroom.fb.com/news/2015/12/community-support-fyi-improving-the-names-process-on-facebook/

Papacharissi, Z. (2010, August). Privacy as a luxury commodity. *First Monday*, p. 15.

Perrin, A. (2015). Social Media Usage: 2005-2015. Retrieved from http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

Pitkänen, O., & Tuunainen, V. K. (2012). Disclosing personal data socially—An empirical study on Facebook users' privacy awareness. *Journal of Information Privacy & Security*, *8*, 3–29. doi:10.1080/15536548.2012.11082759

Priest, M. (1998). The privatization of regulation: Five models of self-regulation. *Ottawa Law Review*, *29*, 233–302.

Scoglio, S. (1998). *Transforming privacy: A transpersonal philosophy of rights*. Westport, CT: Praeger.

Seybert, H., & Reinecke, P. (2013). *Internet use statistics—Individuals: Three quarters of Europeans used the Internet in 2013*.

Silbey, S. S. (2005). After Legal Consciousness. *Annual Review of Law and Social Science*, *1*, 323–368. doi: 10.1146/annurev.lawsocsci.1.041604.115938

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Stewart, D. W., & Shamdasani, P. N. (1990). *Focus groups: Theory and practice*. London, England: SAGE.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Newbury Park, CA: SAGE.

Trottier, D., & Lyon, D. (2011). Key features of social media surveillance. In C. Fuchs, K. Boersman, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of*

Web 2.0 and social media (pp. 89–105). London, England: Routledge.

Turow, J., Draper, N., & Hennessy, M. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Walsh, D., Parisi, J. M., & Passerini, K. (2015). Privacy as a right or as a commodity in the online world: The limits of regulatory reform and self-regulation. *Electronic Commerce Research, 15*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*, 193–220. Retrieved from http://www.jstor.org/stable/1321160

Yang, H. (2013). Young American consumers' online privacy concerns, trust, risk, social media use, and regulatory support. *Journal of New Communications Research*, *5*, 1–30.

Zimmer, M. (2014, February 3). Mark Zuckerberg's theory of privacy. *The Washington Post*. Retrieved from https://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html

Author Biographies

Katharine Sarikakis (PhD, Glasgow Caledonian University) is a Professor of Media Governance, Organisation and Media Industries and Jean Monnet Chair of European Media Governance and Integration in the Department of Communication at the University of Vienna, Austria. Her research interests include the legal and political processes of media and communications governance, including privacy, copyright, diversity, and public service.

Lisa Winter (Doctoral Candidate, University of Vienna) is a Researcher in the Department of Communication at the University of Vienna, Austria. Her research interests include social media and understandings of privacy.