Ethics Inf Technol (2015) 17:89–101
DOI 10.1007/s10676-015-9363-z

ORIGINAL PAPER

Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data

Gordon Hull[1]

Published online: 29 May 2015

Abstract The "privacy paradox" refers to the discrepancy between the concern individuals express for their privacy and the apparently low value they actually assign to it when they readily trade personal information for low-value goods online. In this paper, I argue that the privacy paradox masks a more important paradox: the self-management model of privacy embedded in notice-and-consent pages on websites and other, analogous practices can be readily shown to underprotect privacy, even in the economic terms favored by its advocates. The real question, then, is why privacy self-management occupies such a prominent position in privacy law and regulation. Borrowing from Foucault's late writings, I argue that this failure to protect privacy is also a success in ethical subject formation, as it actively pushes privacy norms and practices in a neoliberal direction. In other words, privacy self-management isn't about protecting people's privacy; it's about inculcating the idea that privacy is an individual, commodified good that can be traded for other market goods. Along the way, the self-management regime forces privacy into the market, obstructs the functioning of other, more social, understandings of privacy, and occludes the various ways that individuals attempt to resist adopting the market-based view of themselves and their privacy. Throughout, I use the analytics practices of Facebook and social networking sites as a sustained case study of the point.

Keywords Privacy · Social networking · Facebook · Foucault · Biopolitics · Neoliberalism · Big data

People say that they value their privacy. However, when they are offered the opportunity to trade private, personal information for immediate but minor benefits such as access to a website, they routinely do so. Young people appear to value privacy even less, constantly uploading revealing material about themselves and others to widely-accessible social media sites like Facebook. This so-called "privacy paradox" is frequently interpreted to prove that people do not, in fact, care about privacy so much after all. However, sociological research shows not only that people—including young people—assign importance to privacy, but also that they routinely engage in complex privacy-protective behaviors (see, e.g., the discussion and references in Marwick and Boyd 2014). If this is the case, then we confront a different privacy paradox. First, how is it that the socially standard regimes of privacy protection featured in "notice and consent" policies and other examples of "privacy self-management" so completely fail to represent how individuals actually conceptualize and attempt to manage their privacy? Second, given the totality of their failure, why are they so persistently taken to present a normatively adequate understanding of privacy?

In what follows, I will use the work of Michel Foucault, in particular his later work on ethics and subjectivity, to argue that privacy self-management regimes need to be

✉ Gordon Hull
ghull@uncc.edu

[1] University of North Carolina Charlotte, 9201 University City Blvd., Charlotte, NC 28223, USA

understood as what I will call a "successful failure."[1] That is, their failure to protect privacy tells only half the story. The other half of the story is their success in establishing a very specific model of ethical subjectivity. Specifically, I will argue that the current reliance on privacy self-management, epitomized by notice and consent regimes, not only completely fails to protect privacy, but that it does so in a way that encourages adherence to several core neoliberal techniques of power: the belief that privacy can only be treated in terms of individual economic choices to disclose information; the occlusion of the fact that these choices are demonstrably impossible to make in the manner imagined; and the occlusion of the ways that privacy has social value outside whatever benefits or losses may accrue to individuals. In Foucaldian terms, that is, privacy self-management functions as a technology of neoliberal governance, by inculcating the belief that subjectivity and ethical behavior are matters primarily of individual risk management coupled with individual responsibility for poorly-managed risks.

The paper proceeds as follows. In the first part, I offer a synthetic presentation of some of the problems with privacy self-management as a model of privacy. The goal is to offer an immanent critique in the sense that the problems with privacy self-management are entirely predictable using the economic tools that are also used to defend the theory. In the second, I outline the social benefits of privacy, and suggest how notice and consent not only occludes, but actively subverts those benefits. The third section places the first two in the context of Foucault's late work on governmentality and ethics, to show how notice and consent can fail to protect privacy, but succeed spectacularly as a strategy of subjection. Throughout, I will use social networking software (and Facebook specifically) as a lead example of the interaction between privacy self-management and subjectification.

Why we have a privacy paradox: the failure of privacy self-management

In the U.S., the standard strategy for protecting privacy online is self-management, usually by way of "notice and consent" to a statement of terms of service or an End User License Agreement (EULA).[2] These contracts stipulate

[1] Foucault's work occupies a strange place in the study of privacy. On the one hand, his discussion of panopticism in *Discipline and Punish* (1977) arguably provided the organizing metaphor for an entire literature around surveillance, even if there has been a move over the last decade to Deleuze (see, e.g., Haggerty 2006; Haggerty and Ericson 2000; Lyon 2006). On the other hand, if one considers "privacy" as an ethical norm or legal right, Foucault is nearly entirely absent from the discussion (notable exceptions are Boyle 1997; Cohen 2013; Reiman 1995). This is no doubt due, in part, to the general treatment of privacy as a question of information disclosure by individuals (which makes the more sociological analysis of panopticism seem less immediately relevant), and to the subsequent adoption of a theory of decisional autonomy that Foucault rejected. For both of these, see the complaint in Cohen (2012a). What is lost in the reduction of Foucault to panopticism and privacy to formal autonomy is Foucault's post *Discipline and Punish* work on techniques of governance, biopolitics, and the formation of ethical subjects. As a whole, this body of work treats the ways that various social practices contribute to a process of "subjection" (or "subjectification"), and, in so doing, how they help to make us who we are. There is considerable discussion about the compatibility of these phases of Foucault's work with each other. In particular, many Foucault scholars e.g., (McNay 2009) think—generally to their frustration – that the later work on ethics is incompatible with, or at least on a completely different footing from, the work on biopolitics and governmentality. Foucault himself famously denied this charge ("it is not power, but the subject, which is the general theme of my research" for the past 20 years (1982, pp. 208–209). For a supportive assessment of Foucault on the point, see Lazzarato (2000). It is also possible that Foucault's understanding of biopower changes between his introduction of the subject in 1976 and his later usage of it (for exemplary treatments, see Collier 2009; Protevi 2010). I will not attempt to resolve either debate here; for the sake of this paper, I will assert but not defend the view that the ethical "techniques of the self" open a path for studying the ways that biopolitics secures its own operation in the individual persons who use these techniques. Foucault's studies of ancient Greek strategies for subjection, then, can be understood as models for studying the techniques in current society. Prima facie plausibility of this view comes from (a) Foucault's own assertions (see above); (b) the extent to which the disciplinary techniques featured in *Discipline and Punish* are precisely about convincing individuals how they should view themselves as subjects of power; and (c) Foucault's emphasis in his discussion of American neoliberalism (Foucault 2008) on the attempt to reconfigure subjectivity along entrepreneurial lines. For discussion of this last point, see, e.g., (Hamann 2009).

[2] I draw the term "privacy self-management" from (Solove 2013). Privacy self-management is essentially the current version of privacy as "control" over personal information, as found in earlier sources such as Westin and (Fried 1968). Early version of the theory included significant attention to sociological literature that described privacy in terms of social group formation. For the ways that this attention diminished, especially in the construction of the argument in Westin, see (Steeves 2009). Complaints about the ubiquity of privacy self-management and its failures are common; in addition to Solove, see, e.g., (Cohen 2012a, 2013; Nissenbaum 2010).

The situation in Europe is, at least on its face, quite different: the EU Data Protection Directive encodes a number of substantive privacy norms, which result in sector-specific differences from U.S. law [for a comparative discussion of healthcare, for example, see (Francis 2014–2015)]. The Directive is also currently undergoing an upgrade designed to update and strengthen the Directive into a Regulation (General Data Protection Regulation, GDPR). There is considerable skepticism, however, as to whether this process will succeed. Bert-Japp Koops (2014), for example—citing some of the same sources discussed here, such as Solove (2013)—argues that the proposed regulation relies too much on consent and its underlying value of autonomy. He also notes that the GDPR in its current version is extraordinarily complex, which reduces the likelihood that it will achieve effective protection, especially insofar as the complexity becomes a barrier to companies viewing privacy as a social value, rather than a compliance-based hoop a similar complaint is made in (Blume 2014). Thus, although considerations of space preclude the

that users of the program or service consent to certain uses of personal information that they make available about themselves. The theoretical defense of privacy self-management accordingly depends both on the assumption that individuals behave rationally (in the economic sense) when they express privacy preferences and on the idea that their behavior adequately reveals those preferences. Unfortunately, neither assumption is true. There are numerous good critiques of the self-management regime; my effort here is to offer something brief and synthetic. Here are three types of reasons why self-management can be expected to underprotect privacy: (1) users do not and cannot know what they are consenting to; (2) privacy preferences are very difficult to effectuate; and (3) declining to participate in privacy-harming websites is increasingly not a viable option for many.[3]

Information deficits and asymmetries

For consent to be meaningful, an individual has to know what she is consenting to. Unfortunately, users are on the wrong end of a substantial information asymmetry, and there is there is good evidence that consumers neither know nor understand the uses to which their data can be put (McDonald and Cranor 2010). No doubt this is in part because privacy statements are notoriously difficult to read, and there is a substantial literature on the complexity of privacy statements and possible ways to make them more accessible. Nonetheless, there are real limits to that sort of reform for at least three reasons. First, websites have every incentive to keep privacy policies as vague as possible, and to reserve the right to unilaterally modify them at will according to business needs. This is particularly true of sites like Facebook, where the "product is access to individuals who have entered personal information" (Hoofnagle and Whittington 2014, p. 628; for a list of what Facebook allows third parties to do, see 630–631). Second, sites freely sell information to third parties, subjecting users to the third party's privacy policy, which of course those users never see. Finally, as I will discuss in the next section, detailed and clear privacy policies themselves impose a burden.

Indeed, even if privacy statements could be made perfectly lucid, substantial information asymmetry problems would still exist:

> Despite lengthy and growing terms of service and privacy, consumers enter into trade with online firms with practically no information meaningful enough to provide the consumer with either ex ante or ex post bargaining power. In contrast, the firm is aware of its cost structure, technically savvy, often motivated by the high-powered incentives of stock values, and adept at structuring the deal so that more financially valuable assets are procured from consumers than consumers would prefer (Hoofnagle and Whittington 2014, pp. 640–641).

That is, the problem of information asymmetry is structural, and cannot be remedied by supplying individuals with more information about sites' privacy policies.

Discussion of information asymmetry at the moment of consent also risks obscuring a more fundamental problem, which is that data mining conspires to make consent meaningless because the uses to which data will be put are not knowable to the user—or perhaps even the company—at the time of consent.[4] Some of these uses will be beneficial, no doubt, but they could also be harmful. Users are in no position to assess either the likelihood or nature of these future uses; in economic terms, this means that these decisions are made in conditions of uncertainty, and are accordingly not easily amenable to risk assessment (Grossklags and Acquisti 2007). Credit card companies have been innovators in such usage of data mining and other analytics, and can serve as an initial illustration of the point. For example, Canadian Tire studied its cardholders and discovered that buying felt pads to keep one's furniture from scuffing the floor predicted being a good credit risk; on the other hand, nearly half of cardholders who used their cards at Sharxx Pool Bar in Montreal missed four payments in a year (Duhigg 2009). Another study concluded that obesity was associated with credit delinquency—up to 14 points over the population-wide baseline for the extremely obese (and three points for the merely overweight). Even after controlling for potentially confounding risk factors, obesity mattered much more for credit delinquency than either recent marriage dissolution or disability (Guthrie and Sokolowsky 2012).

Footnote 2 continued
extension of the discussion into the details of EU law, it seems plausible that at some of the same problems are present there as well.

[3] Although I will not pursue the point in detail, these problems are also problems for technical solutions that depend on predelegating privacy decisions to some sort of data vault or other software agent that encodes users' data and their privacy preferences and then attempts to automatically negotiate with websites and other service providers. Assuming that websites would comply with such an approach on the part of users—and this seems like an assumption that needs independent justification since, as I will note, companies like Facebook clearly make it difficult to protect one's privacy on purpose—software agents could at most help with the difficulty in effectuating privacy preferences. The information asymmetries and uncertainty surrounding privacy decisions cannot be relieved by having a software agent, and setting the agent to refuse to disclose information may still carry unacceptable costs for users. Further, the use of agents only reinforces the idea that privacy is an alienable market good, entrenching the consent mindset.

[4] This is not a new concern: see, for example, (Tavani 1998).

These sorts of analytics have made their way to Facebook, which because of its enormous user base and wealth of personal information, presents a tremendous opportunity for data mining. In 2014, the company triggered an enormous backlash by publishing research indicating that reception of negatively (or positively) coded information from one's newsfeed tended to cause users to express themselves more negatively (or positively). In other words, the well-known "emotional contagion" effect did not require direct, interpersonal interaction (Kramer et al. 2014). Most of the objections centered around the study's method, which subtly manipulated the newsfeed of millions of users for a period of time. On the one hand, as Boyd (2014) points out, some of this criticism is difficult to understand, since consumers routinely accept Facebook's opaque manipulation of their newsfeed. On the other hand, however, users had no reason to expect that this particular manipulation of their newsfeed was coming (and they certainly did not actively consent to participate in that specific study), and they have no way of knowing whether the results of the study will benefit or harm them. In any case, this is hardly the first time Facebook's data has been the basis for analytics. For example, one (in)famous early study (Jernigan and Mistree 2009) found that the percentage of a given user's Facebook friends who identified as gay was strongly correlated with his own sexual orientation – even if he did not disclose it. It was thus relatively simple to out people on Facebook.

More recently, one study (Kosinski et al. 2013) reported that automated analysis of FB "Likes" predicted race (African-American or Caucasian) with 95 % accuracy, and gender with 93 % accuracy. It also correctly classified Christians and Muslims (82 %), Democrats and Republicans (85 %), sexual orientation (88 % for males, 75 % for females), and substance abuse (73 %). Furthermore:

> Individual traits and attributes can be predicted to a high degree of accuracy based on records of users Likes …. For example, the best predictors of high intelligence include "Thunderstorms," "The Colbert Report," "Science," and "Curly Fries," whereas low intelligence was indicated by "Sephora," "I Love Being A Mom," "Harley Davidson," and "Lady Antebellum." Good predictors of male homosexuality included "No H8 Campaign," "Mac Cosmetics," and "Wicked The Musical," whereas strong predictors of male heterosexuality included "Wu-Tang Clan," "Shaq," and "Being Confused After Waking Up From Naps."

Even one Like could have "non-negligible" predictive power. Although the epistemic value of such correlations can and should be challenged (Boyd and Crawford 2012), highly predictive personality traits could also be inferred from Likes:

> For example, users who liked the "Hello Kitty" brand tended to be high on Openness and low on "Conscientiousness," "Agreeableness," and "Emotional Stability." They were also more likely to have Democratic political views and to be of African-American origin, predominantly Christian, and slightly below average age.

And so it goes. It is hard to understand how disclosing one's affection for Hello Kitty implies consent later to disclose possible emotional instability, since that correlation was unknowable to the user (and possibly to anyone at all) at the time of consent. Analyzing actual content may not even be necessary; one study reports that network analysis alone (i.e., looking only at metadata) was able to identify someone's spouse 60 % of the time, concluding that "crucial aspects of our everyday lives may be encoded in the network structure among our friends" if we know how to look (Backstrom and Kleinberg 2014). Even failure can be informative, and the same study noted that when the analysis failed to correctly identify a romantic partner, the relationship was significantly more likely to end 2 months later.

Users might further worry about the uses to which such newly-minted information might be put (for a sobering discussion, see Pasquale 2015). Warnings about exposure to stalking, identity theft and the like have been a regular feature of critical discussions of social networking for some time (see, e.g., Gross and Acquisti 2005; Jones and Soltren 2005), but some specific examples can serve to underscore the disturbing possibilities of privacy harms, as well as their unexpected nature. To return to Hello Kitty, MedBase2000 will sell you a list of "Anxiety and Anxiety Disorder Sufferers" for $79 per 1000 names (cited in Harcourt 2014, p. 24), and the authors of the Likes study propose that the "relevance of marketing and product recommendations could be improved by adding psychological dimensions to current user models," and cite as an example that insurance products could emphasize security when marketing to the emotionally unstable but potential threats to the stable (Kosinski et al. 2013, p. 4). Perhaps more disturbingly, Zeynep Tufekci (2014) reports an internal Facebook study that discovered that subtle 'go and vote' reminders slightly but significantly increased election turnout, in amounts more than sufficient to swing a close election. If FB or another major internet platform were to direct such messages only to voters likely to support candidates receptive to whatever policy objectives the company favored, the temptation would be there to engage in such "digital gerrymandering."

Companies can also use even very simple data to enable disturbing offline behavior by others. For example, the iPhone App GirlsAroundMe (eventually removed by

Apple) scraped Facebook profiles and FourSquare location data to let users (in the terms advertised on its website) "see where nearby girls are checking in, and show you what they look like, and how to get in touch." In case users hadn't already thought the matter through, the site helpfully adds, "in the mood for love, or just for a one-night stand? GirlsAroundMe puts you in control."[5] Beyond the commodification of non-consenting women presented by this App, Hoofnagle and Whittington note that such "enhancing" of data is a readily available strategy online: if a user can be induced to share some information with a site (especially name and zip code), the site can then purchase information about her that she refused to provide (2014, pp. 631–634).

In sum, users do not and cannot plausibly be expected to know enough—neither about the uses to which their information might be put, nor about the specific benefits and harms that might result from those uses, nor about the likelihood that such harms might result—for consent to be meaningful, especially if one makes the assumption that those users are following a risk/benefit model of economic rationality. Even to make that assumption requires the tools of behavioral economics, which can attempt to preserve the assumption of risk/benefit behavior by providing explanation for apparent deviations from that model (for example, hyperbolic discounting of the future, which suggests that individuals will undervalue distant harms compared to those in the present or near future). It is, however, unclear what cognitive biases and heuristics are in play at any given moment.[6] Additionally, as I will indicate in the third section, behavioral economics poses its own set of problems.

In sum, the epistemic problems faced by users are significant enough that Katherine Strandburg suggests that the entire analogy to purchasing a good with one's information is misplaced; "better than the analogy to a purchase transaction would be an analogy to obtaining free medical care in exchange for participating in a trial of a new medical treatment" (Strandburg 2013, p. 151). In particular, she underscores how hard it is for users to measure the disutility associated with any given notice and consent transaction:

> For an Internet user to weigh the costs and benefits of a particular online activity, the user must estimate the marginal expected disutility of the particular data collection associated with that activity. To determine marginal disutility, an Internet user must have information about how the incremental data collected in association with the particular activity changes the overall availability of information about her in the online ecosystem. Not only that, she must be able to connect that increment in available information to an increment in expected disutility. This is essentially an impossible task (2013, pp. 147–148).

Difficult to actualize preferences

People may have difficulty effectuating their privacy preferences. This problem is endemic on sites like Facebook, and it is not obviously the fault of users: successful navigation of the site's constantly changing privacy policies requires a commitment to continually mastering and remastering byzantine detail and complexity. The only seemingly consistent rule is that the software will default to openness.[7] Empirical research repeatedly demonstrates that Facebook users do not successfully effectuate their privacy preferences, and that they often do not even know this. For example, one recent study found that a full third of Facebook users left privacy settings at their open-sharing default, and that nearly two-thirds have actual privacy settings that do not match what they think those settings are—almost invariably in the direction of more disclosure (Liu et al. 2011). Another, which collected data from Columbia University students, found that:

> 93.8 % of participants revealed some information that they did not want disclosed. Given our sample, it is virtually certain that most other Facebook users have similar problems. On the other hand, we note that 84.6 % of participants are hiding information that they wish to share. In other words, the user interface design is working against the very purpose of online social networking. Between these two figures, every single participant had at least one sharing violation. Either result alone would justify changes; taken together, the case is quite compelling (Madejski et al. 2011, p. 11).

In other words, FB's interface design consistently frustrates users' ability to achieve their privacy objectives.[8]

[5] GirlsARoundMe.com, visited 6/2014. There is a periodic reference to "guys" in the site's front page, but it mainly proves its own exceptional status: the pictures are all of women.

[6] For behavioral economics and privacy, see particularly the work of Allesandro Acquisti, e.g., (Acquisti 2009; Grossklags and Acquisti 2007).

[7] Defaults matter. Research indicates that most individuals do not change software or other defaults (as, for example, 401(k) participation, which can be raised dramatically by simply switching from an opt-into an opt-out default). The reasons for this are partly economic—changing defaults (especially on Facebook) takes time and effort, and partly normalizing: the default setting communicates what an "average" or "reasonable" user ought to prefer. See (Shah and Kesan 2007).

[8] One study found that nearly a quarter of respondents regretted mistaken oversharing on Facebook, reporting loss of important relationships and employment (Wang et al. 2011). In an earlier paper,

Conversely, too many opportunities for consent can themselves make it more difficult for users to effectuate their privacy preferences.[9] One study concluded that if all web users were simply to read (once) the privacy policies of the sites they visit, they would each spend about 244 h a year on the task, more than six work-weeks. That diversion would cost the U.S. economy something on the order of $781 billion annually in lost time, and the calculation did not include any time for comparison shopping among privacy policies, a requirement for any claim that markets could develop to satisfy user privacy preferences (McDonald and Cranor 2008). Sites also appear to actively exploit this time commitment to make it more difficult to opt-out of information sharing. According to one recent report (Albergotti 2014), for example, Facebook now allows users to opt-out of sharing their information with data brokers. This seems good, but there is no global opt-out; users must instead right-click on individual ads, visit an external site, and follow that site's opt-out procedure. Also, apparently, the opt-out preference is stored in a cookie on the user's machine, so the ordinarily-privacy-protective act of deleting cookies perversely removes that bit of privacy. Finally, and of course, the opt-out arrived at the same time as Facebook's decision to use its users' web-browsing histories as part of its formula for ad targeting.

The choice isn't really "free"

All but the most formalistic models of consent recognize that nominally uncoerced choices can nonetheless be so constrained that it is difficult to call them "free." The problem is when the cost of exercising a choice becomes too high for someone reasonably to bear. In other words, it needs to be reasonable to forego whatever benefit the user loses to keep her privacy. As more and more of life moves online, and as more and more websites condition access on various forms of tracking, it will become increasingly difficult to resist information disclosure. Specifically, Facebook use has been tied to college students' social capital for several years now; asking a student to forego Facebook in order to preserve her privacy is putting a high and increasing price on privacy preservation (Ellison et al. 2007). The difficulty is not just online, as the finding that Facebook users use the program to maintain offline relationships is robust (Lampe et al. 2008), and recent studies document the extent to which for college students in particular (who are also heavy users of mobile technology, including to access Facebook), "Facebook is probably, even more than other communication means, the glue in many students' life" because it facilitates casual offline interactions for a population that leads "socially complex, nomadic lives" (Barkhuus and Tashiro 2010, p. 140).

Although a lot of the research and attention around social media has centered on college students in the U.S., it should be noted that its importance in other contexts is increasing as well. For example, there is evidence that Iraqi civilians used Facebook to maintain and develop safe social interactions (including religiously mandated interactions with relatives during Ramadan) when actual trips outside of the home were too dangerous to undertake (Semaan and Mark 2012). These are the sorts of benefits users have to forego to maintain their privacy.

Privacy as a social value

Privacy is not just an individual value. It is also a social value: a society in which some level of privacy is present is better not just for the individuals who assign value to their privacy, but for everyone else too. In economic terms, privacy protection has positive externalities that are not captured by privacy self-management, and which are often at odds with it. Of the social value of privacy, Dan Solove writes:

> Society involves a great deal of friction, and we are constantly clashing with each other. Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocating, and it might not be a place in which most would want to live. When protecting individual rights, we as a society decide to hold back in order to receive the benefits of creating the kinds of free zones for individuals to flourish (Solove 2007, p. 762).

Most basically, Dourish and Anderson emphasize that privacy functions both to set group boundaries—possessing private information is a marker of inclusion in a group, and often functions independently of the content of that information—and to define (with security), what risks a social group considers tolerable (Dourish and Anderson 2006). Privacy, in short, is essential to the maintenance of the social networks within which individuals can flourish.

Research on Facebook underscores the gap between these social practices and privacy self-management. This research indicates that individuals are at least partially motivated by normative social considerations, even if they do not clearly see the connection between sharing with

Footnote 8 continued
two colleagues in human–computer interaction and I made the case that FB's privacy problems are design-related: see (Hull et al. 2011). For more on the HCI implications of privacy, see, for example, (Dourish and Anderson 2006).

[9] For a theoretical development of this concern, see (Schermer et al. 2014).

friends on Facebook and sharing with Facebook. That is, users try to preserve privacy norms in their social dealings with one another, but seem less concerned to protect their privacy against Facebook (Raynes-Goldie 2010; Young and Quan-Haase 2013). One study reported that users were concerned not to overshare, both out of a sense of modesty and out of a desire not to burden even close ties with excessive communications (Barkhuus 2012). Another noted that student perceptions of the appropriateness of sharing particular information in SNS depended on their perception of whether the context was private or public (Bazarova 2012). Students also expressed a strong norm against showing up, unannounced, based on a posting of location data (Barkhuus and Tashiro 2010, p. 138). These results suggest that privacy practices on the ground are highly granular and context-sensitive. Users also attempt to circumvent some of the data-sharing affordances of SNS software, as I note in the final section. Taken together, this evidence indicates a real disconnect between privacy self-management theory and how privacy actually functions; *i.e.*, that "social factors rather than concerns about a company's privacy practices may be the primary factor that influences disclosure behavior" (King et al. 2011, p. 5).[10] Evidence such as this allows one to underscore at least two points: first, it gives the lie to the meme that "young people do not care about privacy." Second, it shows that the notice and consent model, which presents privacy as a purely economic transaction between a user and a service provider, not only does not capture privacy practices, but that it insistence on it accordingly actively occludes those practices.

More broadly, there are other social benefits to privacy as well. Anita Allen, for example, notes that "we need expert advice and a range of competently performed services in order to flourish as citizens" (2011, p. 109; more generally, see 99–122). Most people at some point require the services of a doctor, an attorney, an accountant, a tax preparer, and so forth. Without enforced confidentiality in these relationships, the social purposes they serve (like public health and the smooth functioning of the contract system undergirding the economy) would be undermined. Other social benefits include those surrounding free association; for example, a landmark Supreme Court ruling prevented Alabama from compelling the NAACP to submit its membership lists to the state. Such associational privacy unquestionably protects those in socially disfavored groups (Allen 2011, pp. 123–156). Along the same lines but more broadly, as Julie Cohen (2013) argues, privacy serves at least two vital social functions. First, privacy allows individuals to develop with the independence and space for critical thinking to engage in meaningful civic participation.[11] Second, privacy, and not its absence, turn out to be critical for innovation, since innovation happens when individuals encounter unexpected constraints, situations, and opportunities, and then have the space to tinker and experiment with them.[12]

Additionally, privacy rules and norms have distributional consequences, and these do not always happen in predictable ways (Strahilevitz 2013). One issue is that privacy protection can present a collective action problem in the form of a classical prisoner's dilemma. That is, privacy self-management does not just obscure the social benefits of privacy, it actively subverts them: particularly once certain tipping points are reached, it will almost always be individually rational to forego privacy, even as the social benefits of privacy remain collectively rational. This problem is most strikingly shown in what Scott Peppet calls the "unraveling effect." Peppet proposes that, even if we assume that users retain perfect control over the information they disclose and to whom they disclose it, the economics of data disclosure will tend toward an inexorable reduction of privacy (Peppet 2011). Take Progressive Insurance's "good driver" discount for people who are willing to have tracking devices monitor their driving. Good drivers will have a financial incentive to signal their good driving by volunteering to be monitored. Marginal drivers will soon face powerful incentives to be included with the good drivers, and so they will also volunteer to be monitored. Eventually, even terrible drivers, who have every incentive to avoid monitoring, will be volunteering, in order to avoid the sudden presumption that non-participants have something terrible to hide. The general point is that users at the top of whatever category they are being sorted into often have an economic incentive to signal their superior status. Users near the top then have a reason. And so it goes; eventually, not disclosing information becomes a stigma.

An important feature of the preceding analyses is epistemic: not only are individuals incapable of knowing the economic value of their privacy, either to themselves or to others (as noted in the previous section), but the social

[10] For more evidence of this point—that social norms and social factors like trust among group members—influence disclosure behavior in the context of SNS, see, e.g., (Nov and Wattal 2009). One ethnographic study suggests that users care about social privacy (both engaging in a number of privacy-protective behaviors but also using lax privacy settings to engage in some social surveillance) but not about what Facebook as a company does with their information (Raynes-Goldie 2010). Users also appear to carry social norms from one context into a new one that they perceive to be analogous (Martin 2012).

[11] On this point, see also (Reiman 1995), pointing out that privacy is therefore required for the development of the sort of subject who is able to rationally assess and trade away her privacy.

[12] Cohen's claim about innovation—which flies in the face of orthodoxy—has not gone unchallenged. See,e.g., (Strahilevitz 2013, p. 2040 n125).

benefits of privacy are also both substantial and difficult to quantify. The sort of rationality presupposed by self-management, however, expects individuals to make exactly these sorts of calculations, or at least to believe that they should be making such calculations. Such forced conversion of aleatory, chance moments into risk calculations—the burden for which is borne entirely by those compelled to make them—is a widely recognized feature of neoliberal governmentality in general.[13] Insistence on self-management can distract from more basic questions; as Strandburg (2013) points out, there is actually very little good research that says that data-driven, targeted advertising (where the shoe ad you looked at yesterday follows you around the Web) is any more effective than contextual advertising (where you see Ford ads displayed on a car repair page). Context-based advertising has none of the privacy difficulties of the data-driven approach, and it is a lot cheaper. That has not, of course, slowed the development of increasingly complex targeted models, against the more general backdrop of the neoliberal presentation of the ideal individual as an "entrepreneur of himself," maximizing his expected returns based on calculated risks and investments of his human and other capital (Foucault 2008).

Privacy and subjectification

Notice and consent, then, fails completely as a strategy for privacy protection: it presents users with choices they cannot rationally make, and consistently fails to make legible the many social reasons why privacy is valuable. Rather than focus on privacy self-management as a failure, however, I would like in this section to propose that it serves very well as what Foucault would call a "technique of power." As such, its empirical success in protecting privacy or not is less relevant than the ways it presents an information environment in which individuals see themselves as functioning autonomously, treating personal information as a low-value, purely personal good they can easily trade for other desired goods and services.

The general thesis that our usage of information technologies affects not just what we do, but who we are, has been well-studied in a range of contexts from video games to social media, whether as a medium of communication, or as a place where fundamental social concepts like friendship are negotiated.[14] My choice of Facebook as a case study was in this regard not accidental, because, as the above indicates, Facebook and other SNS are clearly involved in how people develop and maintain their identities, particularly as they engage with others. As Julie Cohen (2012a) has recently argued in extensive detail, the subject who chooses (or not) privacy does not come to her informational environment fully-formed. Rather, subjects are partly constituted by their information environment. Choices about whether to surrender personal information to Facebook will accordingly become a part of who we are; to the extent that Facebook nudges (or shoves) those choices in a particular direction, Facebook is itself an active agent in how we understand and constitute ourselves. Cohen suggests that one area of particular concern is the way that networked environments increasingly rely upon regimes of access control. From the individual's point of view, this often manifests itself as a choice between making oneself increasingly transparent to corporate and governmental entities, or being denied access to something of importance. Every time that we "click here to accept" or otherwise view ourselves as making an autonomous choice in that regard, we further naturalize these regimes, the endpoint of which lies in a mode of governmentality whose objective is not that we desire a particular thing or not, but that we only have the sorts of desires that can be monetized. An important component of this is inculcating the belief that all choices are autonomously made by subjects who emerge fully-grown into an information environment. That is, the belief that subjects are autonomous and exogenous to their information environments serves to occlude precisely the extent to which that environment very carefully molds the sorts of subjects that can emerge within it.

Borrowing terms from Foucault, we need to view these overlapping regimes of authorization and notice and consent as part of a technique of subjectification. "Subjectification" refers to "the different modes by which, in our culture, human beings are made subjects" (Foucault 1982, p. 208). The details of Foucault's understanding of subjectification need not detain us here, but the general point is that human self-understanding (and thus, the "truth" about who we are) is substantially a product of our interactions with various regimes of social, legal, and other forms of

[13] See, e.g., (Amoore 2004) (on the individualization of risk in the workplace); (Binkley 2009) (parenting guides); (Cooper 2012) (increasing contingency of paid work); (Ericson et al. 2000) (disaggregation in insurance); (Feher 2009) (centrality of human capital and notions of entrepreneurship); (Lazzarato 2009) (importance of financialization); (Reddy 1996) (role of expert knowledge); and (Simon 2002) (rise of extreme sports as emblematic). For a very accessible general discussion, see (Brown 2005).

[14] For social networking, see the discussion and cites above. For social networking and robotics, see also (Turkle 2011). For violent video games, see (McCormick 2001; Waddington 2007; Wonderly 2008). I advance the thesis in the context of library filtering programs (2009) and digital rights management (Hull, 2012). It is important to note that one does not have to be a reader of Foucault to arrive at this hypothesis: for the "extended mind" hypothesis and its application to technological environments, see (Clark 2003), and for an argument motivated very much by classical liberalism, see (Benkler 2006).

power, *i.e.*, "the way in which the individual has to constitute this or that part of himself as the prime material of his moral conduct" (Foucault 1985, p. 26). How we achieve this he calls the "mode" of subjection, which is "the way in which the individual establishes his relation to the rule and recognizes himself as obliged to put it into practice" (27).

There are many different ways of achieving this relation; among those most relevant in the context of privacy are recognizing oneself as part of a group that practices certain methods of subjectification. The most obvious instances are the ways that friendship changes as it is mediated online, and that online information facilitates social surveillance of users by one another. But there are more subtle ways, as well. Not only do Facebook users repeatedly accept the sharing of their (and their friends') information with third parties, they are also forced to navigate the complex privacy policies of the site, including (until recently) its complete lack of granularity in characterizing different kinds of "friends." Social networks are segmented differently online and off, and users must be adept at navigating the differences.[15] Users must also develop social rituals for avoiding and managing the inevitable privacy breakdowns. Teenagers on MySpace, for example, tended to have more than one profile—one for parents, and one for friends (Boyd 2007). They also become adept at esotericism, writing mateiral that can be read one way by friends and another by parents (Marwick and Boyd 2014). At an even more fundamental level, the structure of SNS rewards those who disclose information and nudges those who do not to greater disclosures. The point is underscored in a study of Canadian college students, which found that "disclosure … becomes an aspect of identity construction, and that construction is linked with popularity: the people who are most popular are those whose identity construction is most actively participated in by others" (Christofides et al. 2009, p. 343).

Characterizing privacy as a question of formal autonomy and then offering an endless number of opportunities to enact that characterization is then the process of subjectification:

> A moral action tends toward its own accomplishment; but it also aims beyond the latter, to the estalbishing of a moral conduct that commits and individual, not only to other activities always in conformity with values and rules, but to a certain mode of being, a mode of being characteristic of the ethical subject (Foucault 1985, p. 28).

In other words, users are presented with a repeated choice: more privacy or less? Everything about the context of that choice encourages them to answer "less." This in turn habituates them into thinking that less privacy is what normal people want.

At the same time, each iteration of the norm of less privacy further entrenches its status as a norm. To the extent that individuals' privacy decisions are context-dependent, this means that individuals will make fewer privacy-protective decisions. Successful iterations in turn support a larger social narrative that privacy is primarily an antiquated roadblock on the path to greater innovation (Cohen 2013). Even if that narrative is ultimately untrue, it has the further function of neutralizing and depoliticizing the distributional effects of treating users' information as sources of capital accumulation. In other words, it also obscures that transactions aren't even, at the end of the day, about privacy: they are about websites obtaining information which they can then sell to other data brokers (Cohen 2012b). The result is a paradigmatic instance of the operation of power, in the sense given by Foucault, where "it is a total structure of actions brought to bear upon possible actions; it incites, it induces, it seduces, it makes easier or more difficult; in the extreme it constrains or forbids absolutely" (Foucault 1982, p. 220).

In the present context, the various interconnected logics of power construe individuals as primarily economic actors, as instantiations of *homo economicus*. As Foucault (2008) notes, the emergence of American neoliberalism in theorists such as Becker was perhaps most distinctive in its insistence that all aspects of social existence could be modeled on economic cost-benefit analysis. Of course, as the privacy paradox indicates, not all of life seems immediately amenable to such analysis. Behavioral economics, which nuances the model, becomes at this moment a part of the problem because it presents economically irrational behavior as a deviation from correct, rational decision-making. Presenting the deviation as irrational then allows the problem to be packaged as poor risk-modeling by data subjects, who can be nudged into doing better. The process thus repeats the presentation of privacy as an economic decision, both occluding the actual uncertainties users face and offering the possibility of corrective strategies on the part of websites wanting to elicit "rational" behavior.[16] As John McMahon notes, the behavioral economic strategy thus serves to depoliticize social problems. In the present

[15] On this, see, for example (Binder et al. 2009) [finding that "social space provided by SNS typically lacks boundaries and segmentation that are characteristics of offline networks. Boundaries between social spheres occur naturally in offline networks, mostly due to spatial/temporal separation of contacts. This elaborate structure is dropped in online environments" (966)];.

[16] It is true that users can be nudged to more privacy-protective behavior, but when undertaken in the therapeutic terms of behavioral economics, this nudging serves to even further entrench the framing of privacy as a problem for economic rationality.

context, this means both the further erosion of our ability to see privacy as a social and political construct and the further subsumption of social life into markets. As McMahon puts it, "if there is a rationality to the irrationality of economic actors, then the market can respond to, change and/or create incentives to shift behavior" (McMahon 2015, p. 10).

The anxious Facebook user who constantly monitors her online behavior to avoid getting fired thus enacts only one point in a wide set of techniques by which individuals are conditioned to view themselves as both profitably on permanent display, and individually responsible for what others see. This, then, is the real significance of privacy self-management. It is not that it does or does not protect individual privacy; it is that it construes individuals as consumers who make economic decisions about the value of their privacy as an alienable commodity. In so doing, it is part of an apparatus that encourages users to model themselves as economically rational consumers, even in areas (like sharing app games with friends, or, indeed, with regard to "friendship" itself) that one might otherwise not initially appear to be part of the market.[17]

Conclusion: a note about resistance

What, then, of the "privacy paradox," when individuals say they value their privacy, but then behave as if they do not? Foucault proposes that power and resistance always occur together, and proposes that "in order to understand what power relations are about, perhaps we should investigate the forms of resistance and attempts made to dissociate these relations (1982, p. 211). In that vein, it seems to me that one undertheorized way to understand the privacy paradox is as a besieged form of resistance, of an effort, as Foucault puts it, "to refuse what we are" (Foucault 1982, p. 216). Consumer outrage at Facebook's privacy practices, and its research into its users' behavior, such as the emotional contagion survey, is another example; in at least one instance, however, it was sufficient to get a feature (the reviled Beacon) removed (Boyd 2008). One should also note that the resistance is not merely verbal, as people install ad blocking software, delete cookies, and so forth (Hoofnagle and Whittington 2014). As noted above, teenagers go to byzantine lengths to try to protect themselves from surveillance on Facebook, including deleting and undeleting their account to hide it from view when certain individuals are likely to be watching, just as college students laboriously untag themselves from photos after an evening out (Marwick and Boyd 2014). Predictably, corporations actively try to thwart these efforts at self-help: when consumers delete cookies, for example, advertisers hide them in flash videos. Not only does Facebook demand that users be their offline selves on the site, it both makes it notoriously hard to change privacy settings, and it changes the available settings routinely, a practice that dramatically increases the cost of efforts at privacy self-management. As noted above, Facebook users work very hard to protect themselves from social surveillance, but the institutional setting is one that makes it nearly impossible to protect themselves from surveillance by Facebook. Thus they tend toward social strategies like cryptic messaging rather than attempting to navigate the site's privacy settings (Barkhuus 2012). It is no surprise that users appear to have given up on the task of protecting themselves from Facebook, but outrage over Beacon and the emotional contagion study suggests both that users do in fact care, and that the site does a good job making it nearly impossible to achieve meaningful privacy protection against the corporation itself.

Resistance, of course, is not what any official narrative says: we hear instead that, in fact, consumers do not value their privacy. Privacy self-management abets such an official narrative in at least two ways. First, by viewing the loss or preservation of privacy as a commercial transaction, and then treating the transaction as revealing consumer preference, the privacy self-management model obscures a social struggle, repackaging it as a well-functioning market. Both the enthusiastic sharing of information and its grudging release appear as the preference of an economically rational consumer. That is, treating economic rationality as the truth of subjectivity makes it possible to propose that no matter what someone does, it can and should be understood as presenting her revealed preferences. Even more importantly, it assumes that those preferences have been formed autonomously, outside of the context in which they appear.

Second, the very binarization of privacy self-management, with its endless disjunctive share (with everyone) or not (with anyone) contributes to the problem.[18] In Foucauldian-based theory, iterability, the fact that norms have to be repeatedly enacted socially, generates an inevitable resistance. This is most clear in norms having to do with embodiment, as no one actually inhabits "the body," and so the simple fact of living in the world generates a tension between ascribed norms and actual embodied life (Hayles 1999). Analogously, notice-and-consent regimes' erasure

[17] For the argument that the EU GDPR creates similar myths—both that privacy is more protected than it is, and that subjects are more empowered than they are—see (Blume 2014; Koops 2014).

[18] Koops suggests that the proposed EU regulations are stuck in a similar binarism: "EU data protection law applies an all-or-nothing approach: data is either personal data (triggering the whole regime), or it is not (triggering nothing), but it cannot be something in between or something else" (2014, 257).

of the granularity and social embededness of privacy practices works to foreclose that entire sphere of potential resistance: one either accepts the privacy bargain in its entirety, or not. It is as if one's choices for embodiment were between perfectly having the socially prescribed body, or not being embodied at all. This is part of why it is important to look at the actual social practices of Facebook users and the ways they push back against the norms of openness they are asked to iterate. It is also part of why insisting on the evidentiary value of privacy self-management is so pernicious: doing so both actively occludes possibilities for resistance and enables a narrative of consumer preferences based on that occlusion.

It is important to see these subaltern functions of the economization of privacy discourse, even and especially when it is used to explain apparent resistance to further disclosure. To hope to make any progress at all toward protecting privacy, it is important not just to improve users' ability to control their information; it is important to dismantle the epistemic and normative power of the claim that privacy is a matter of individual control of information. As Cohen puts it, "to grapple with the problem of whether information privacy claims are as deeply irrational as they can sometimes appear, we must bring the almost-invisible into critical focus (2012b p. 107). Our model of privacy, and the way it facilitates privacy's inevitable erosion, are part of our problem.

References

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *Security & Privacy, IEEE, 7*(6), 82–85. doi:10.1109/MSP.2009.163.

Albergotti, R. (2014, June 12). Facebook to target ads based on web browsing. *Wall Street Journal*.

Allen, A. L. (2011). *Unpopular privacy: What must we hide?*. Oxford; New York, N.Y.: Oxford University Press.

Amoore, L. (2004). Risk, reward and discipline at work. *Economy and Society, 33*(2), 174–196. doi:10.1080/0308514041000167711.

Backstrom, L., & Kleinberg, J. (2014). *Romantic partnerships and the dispersion of social ties: A network analysis of relationship status on facebook*. Paper presented at the Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing, Baltimore, Maryland, USA.

Barkhuus, L. (2012). The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. *Proceedings of CHI2012 Austin*.

Barkhuus, L., & Tashiro, J. (2010). *Student socialization in the age of facebook*. Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA.

Bazarova, N. N. (2012). *Contents and contexts: Disclosure perceptions on facebook*. Paper presented at the Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work, Seattle, Washington, USA.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven [Conn.]: Yale University Press.

Binder, J., Howes, A., & Sutcliffe, A. (2009). *The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites*. Paper presented at the Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, USA.

Binkley, S. (2009). The work of neoliberal governmentality: Temporality and ethical substance in the tale of two dads. *Foucault Studies, 6*, 60–78.

Blume, P. (2014). The myths pertaining to the proposed general data protection regulation. *International Data Privacy Law, 4*(4), 269–273. doi:10.1093/idpl/ipu017.

Boyd, D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *MacArthur foundation series on digital learning—Youth, identity, and digital media volume*. Cambridge, M. A.: MIT Press.

Boyd, D. (2008). Facebook's privacy trainwreck: Exposure invasion and social convergence. *Convergence, 14*(1), 13–20.

Boyd, D. (2014). What does the Facebook experiment teach us? Retrieved from http://www.zephoria.org/thoughts/archives/2014/07/01/facebook-experiment.html.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society, 15*(5), 662–679. doi:10.1080/1369118x.2012.678878.

Boyle, J. (1997). *Shamans, software and spleens: Law and the construction of the information society*. Cambridge, MA: Harvard University Press.

Brown, W. (2005). *Neoliberalism and the end of liberal democracy edgework: Critical essays on knowledge and politics* (pp. 37–59). Princeton: Princeton University Press.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior, 12*(3), 341–345. doi:10.1089/cpb.2008.0226.

Clark, A. (2003). *Natural-born cyborgs: Minds, technologies, and the future of human intelligence*. Oxford; New York: Oxford University Press.

Cohen, J. E. (2012a). *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven [Conn.]: Yale University Press.

Cohen, J. E. (2012b). Irrational privacy? *Journal of Telecommunications and High Technology Law, 10*, 241–249.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review, 126*, 1904–1933.

Collier, S. J. (2009). Topologies of power: Foucault's analysis of political government beyond 'governmentality'. *Theory, Culture & Society, 26*, 78–108.

Cooper, M. (2012). Workfare, familyfare, godfare: Transforming contingency into necessity. *South Atlantic Quarterly, 111*(4), 643–661. doi:10.1215/00382876-1724120.

Dourish, P., & Anderson, K. (2006). Collective information practice: Emploring privacy and security as social and cultural phenomena. *Human-Computer Interaction, 21*(3), 319–342. doi:10.1207/s15327051hci2103_2.

Duhigg, C. (2009). *What does your credit-card company know about you?*. USA: New York Times Magazine.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x.

Ericson, R., Barry, D., & Doyle, A. (2000). The moral hazards of neoliberalism: Lessons from the private insurance industry.

Economy and Society, 29(4), 532–558. doi:10.1080/03085140050174778.
Feher, M. (2009). Self-appreciation; or, the aspirations of human capital. *Public Culture, 21*(1), 21–41. doi:10.1215/08992363-2008-019.
Foucault, M. (1977). *Discipline and punish: The birth of the prison*. New York: Pantheon Books.
Foucault, M. (1982). The subject and power. In H. L. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: Beyond structuralism and hermeneutics* (pp. 208–226). Chicago: University of Chicago Press.
Foucault, M. (1985). *The use of pleasure* (trans: Hurley, R). New York: Vintage Books.
Foucault, M. (2008). *The birth of biopolitics: Lectures at the Collège de France,* 1978–79 (trans: Burchell, G). New York: Palgrave Macmillan.
Francis, L. (2014–2015). Privacy and health information: The United States and the European Union. *Kentucky Law Journal, 103*, 419–431.
Fried, C. (1968). Privacy. *Yale Law Journal, 77*(3), 475–493.
Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks*. Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA.
Grossklags, J., & Acquisti, A. (2007). What can behavioral economics teach us about privacy? In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. D. C. di Vimercati (Eds.), *Digital privacy* (pp. 363–377). Boca Raton: Auerbach Publications.
Guthrie, K., & Sokolowsky, J. (2012). Obesity and credit risk.
Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 23–45). Cullompton, Devon: Willan Pub.
Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622. doi:10.1080/00071310020015280.
Hamann, T. H. (2009). Neoliberalism, governmentality, and ethics. *Foucault Studies, 6*, 37–59.
Harcourt, B. E. (2014). *Governing, exchanging, securing: Big data and the production of digital knowledge*. Paper presented at the Big data, entreprises et sciences sociales—Usages et partages des données numériques de masse, Paris.
Hayles, N. K. (1999). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. Chicago, Ill.: University of Chicago Press.
Hoofnagle, C. J., & Whittington, J. (2014). Free: Accounting for the costs of the internet's most popular price. *UCLA Law Review, 61*, 606–670.
Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on Facebook. *Ethics and information technology*, *13*(4), 289–302.
Hull, G. (2012). Coding the dictatorship of 'the They:' A phenomenological critique of digital rights management. In M. Sanders & J. J. Wisnewski (Eds.), *Ethics and phenomenology* (pp. 197–220).
Jernigan, C., & Mistree, B. F. T. (2009). Gaydar: Facebook friendships expose sexual orientation. *First Monday, 14*(10).
Jones, H., & Soltren, J. H. (2005). *Facebook: Threats to privacy*. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf.
King, J., Lampinen, A., & Smolen, A. (2011). *Privacy: Is there an app for that?* Paper presented at the Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania.
Koops, B.-J. (2014). The trouble with European data protection law. *International Data Privacy Law, 4*(4), 250–261. doi:10.1093/idpl/ipu023.
Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences,*. doi:10.1073/pnas.1218772110.
Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788–8790. doi:10.1073/pnas.1320040111.
Lampe, C., Ellison, N. B., & Steinfield, C. (2008). *Changes in use and perception of facebook*. Paper presented at the Proceedings of the 2008 ACM conference on computer supported cooperative work, San Diego, CA, USA.
Lazzarato, M. (2000). Du biopouvoir à la biopolitique. *Multitudes, 1*(1), 45–57.
Lazzarato, M. (2009). Neoliberalism in action: Inequality, insecurity and the reconstitution of the social. *Theory, Culture & Society, 26*(6), 109–133. doi:10.1177/0263276409350283.
Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). *Analyzing facebook privacy settings: User expectations vs. reality*. Paper presented at the Proceedings of the 2011 ACM SIGCOMM conference on internet measurement conference, Berlin, Germany.
Lyon, D. (Ed.). (2006). *Theorizing surveillance: The panopticon and beyond*. Cullompton, Devon: Willan Pub.
Madejski, M., Johnson, M., & Bellovin, S. E. (2011). The failure of online social network privacy setetings *Columbia University Computer Science Technical Reports*.
Martin, K. (2012). Information technology and privacy: Conceptual muddles or privacy vacuums? *Ethics and Information Technology, 14*(4), 267–284. doi:10.1007/s10676-012-9300-3.
Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society,*. doi:10.1177/1461444814543995.
McCormick, M. (2001). Is it wrong to play violent video games? *Ethics and Information Technology, 3*(4), 277–287. doi:10.1023/a:1013802119431.
McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. I/S. *A Journal of Law and Policy for the Information Society, 4*(3), 540–565.
McDonald, A. M., & Cranor, L. (2010). *Americans' attitudes about internet behavioral advertising practices*. Paper presented at the Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, Chicago, Illinois, USA.
McMahon, J. (2015). Behavioral economics as neoliberalism: Producing and governing *homo economicus*. *Contemporary Political Theory, 14*, 137–158.
McNay, L. (2009). Self as enterprise: Dilemmas of control and resistance in Foucault's the birth of biopolitics. *Theory, Culture & Society, 26*(6), 55–77.
Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto: Stanford University Press.
Nov, O., & Wattal, S. (2009). *Social computing privacy concerns: Antecedents and effects*. Paper presented at the Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, USA.
Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.
Peppet, S. R. (2011). Unraveling privacy: The personal prospectus and the threat of a full disclosure future. *Northwestern Law Review, 105*(3), 1153–1204.
Protevi, J. (2010). What does Foucault think is new about neoliberalism?. *Pli: Warwick Journal of Philosophy, 21*.
Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1).

Reddy, S. G. (1996). Claims to expert knowledge and the subversion of democracy: The triumph of risk over uncertainty. *Economy and Society, 25*(2), 222–254. doi:10.1080/03085149600000011.

Reiman, J. H. (1995). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal, 11*(1), 27–44.

Schermer, B., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology, 16*(2), 171–182. doi:10.1007/s10676-014-9343-8.

Semaan, B., & Mark, G. (2012). *'Facebooking' towards crisis recovery and beyond: Disruption as an opportunity*. Paper presented at the Proceedings of the ACM 2012 conference on computer supported cooperative work, Seattle, Washington, USA.

Shah, R. C., & Kesan, J. P. (2007). *Governing with information technologies*. Paper presented at the Proceedings of the 8th annual international conference on Digital government research: Bridging disciplines \& domains, Philadelphia, Pennsylvania.

Simon, J. (2002). Taking risks: Extreme sports and the embrace of risk in advanced liberal societies. In T. Baker & J. Simon (Eds.), *Embracing risk: The changing culture of insurance and responsibility* (pp. 177–208). Chicago: University of Chicago Press.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review, 44*, 745–772.

Solove, D. J. (2013). Privacy Self-management and the consent dilemma. *Harvard Law Review, 126*, 1880–1903.

Steeves, V. (2009). Reclaiming the social value of privacy. In I. Kerr, C. Lucock, & V. Steeves (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 191–208). Oxford: Oxford University Press.

Strahilevitz, L. J. (2013). Toward a positive theory of privacy law. *Harvard Law Review, 126*, 2010–2042.

Strandburg, K. J. (2013). Free fall: The online market's consumer preference disconnect. *University of Chicago Legal Forum, 2013*, 95–172.

Tavani, H. T. (1998). Informational privacy, data mining, and the internet. *Ethics and Information Technology, 1*(2), 137–145. doi:10.1023/a:1010063528863.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday, 19*(7).

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*.

Waddington, D. (2007). Locating the wrongness in ultra-violent video games. *Ethics and Information Technology, 9*(2), 121–128. doi:10.1007/s10676-006-9126-y.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). *"I regretted the minute I pressed share": A qualitative study of regrets on Facebook*. Paper presented at the Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania.

Wonderly, M. (2008). A Humean approach to assessing the moral significance of ultra-violent video games. *Ethics and Information Technology, 10*(1), 1–10. doi:10.1007/s10676-007-9149-z.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on facebook. *Information, Communication & Society, 16*(4), 479–500. doi:10.1080/1369118X.2013.777757.