THE INFORMATION SOCIETY
2016, VOL. 32, NO. 1, 51–63
http://dx.doi.org/10.1080/01972243.2015.1107166

Routledge
Taylor & Francis Group

Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop?

Kirsten Martin

Department of Strategic Management and Public Policy, George Washington University, Washington, DC, USA

ABSTRACT

The goal of this article is to examine the strategic choices of firms collecting consumer data online and to identify the roles and obligations of the actors within the current network of online tracking. In doing so, the focus shifts from placing the onus on individuals to make an informed choice, to justifying the roles and responsibilities of firms when gathering, aggregating, and using consumers' interests or behavior online. Firms online are uniquely positioned to undercut or to respect privacy expectations within three possible roles: as a member of a supply chain of information traders, within a network of surveillance online, and as an arm of law enforcement. These firms benefit from aggregating and analyzing consumer data and have an associated responsibility to not only minimize the harm to consumers but also to enact change where the firm is in the most knowledgeable and powerful position.

ARTICLE HISTORY
Received 7 August 2014
Accepted 3 May 2015

KEYWORDS
Big data; business ethics; Internet; privacy; surveillance; tracking online

Through everyday activities, such as buying groceries, paying bills, researching medical symptoms, and mapping runs, consumers create a data trail that is collected by companies and aggregated for later use. The term "big data" refers to the marriage of modern predictive tools with these large data sets of consumer information (boyd and Crawford 2012; Lohr 2012; Sloan and Warner 2014). Better analytical capabilities and larger data sets—with greater volume, variety, and velocity (Laney 2001)—allow for greater precision in tracking individuals and more widespread, beneficial use of big data by firms, such as for fraud prevention and credit risk assessments (Beales and Muris 2008; U.S. Senate 2013), as well as in health care, mobile, smart grids, traffic management, retail, and payment services (Tene and Polonetsky 2013).

While recent advances have led to a democratization of becoming a "captive audience" without functional opt-out mechanisms, thereby making notice and choice less meaningful (Popescu and Barah 2013). Privacy law scholars Schwartz and Solove (2011) summarize the idea behind notice and choice: As long as a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected.

The emergence of widespread consumer tracking compounds the frailty of relying on notice and choice to govern privacy online. Currently, the only affirmative responsibility of firms online is adequate notification (Calo 2012; Beales 2013). Firms online are not responsible for their specific privacy practices—only in communicating their tactics to consumers. In focusing on disclosure as

identify the roles and obligations of the actors within the current network of online tracking. In doing so, the focus shifts from placing the onus on individuals to make an informed choice to justifying the roles and responsibilities of firms when gathering, aggregating, and using consumers' movements, preferences, interests, or behavior online. Firms are uniquely positioned to undercut or to respect expectations on privacy based on the information tracked and the firms' relationship with users.

The article proceeds as follows. First, I categorize firms online based on the two important strategic decisions concerning (1) a firm's relationship with consumers and (2) the breadth of information collected. Second, these strategic choices are framed as positioning firms to either undercut or respect privacy expectations within three possible overlapping roles: as a member of a supply chain of information traders, within a network of surveillance online, and as an arm of law enforcement. Based on the firms' strategic position online, I identify the moral basis for firms' obligations for each role and summarize in Table 1.

Strategic choices of firms online

When online, firms regularly gather and store consumers' information, browsing habits, clickstream data, and purchasing history. While websites have long been known to record users' online activities in order to suggest products or give discounts, additional actors and technologies have entered the online tracking space with increasing access to user information. For example, a Web beacon can capture detailed information such as clicking, typing, and browsing behavior and then relay that information to professional tracking companies and data aggregators; a mobile software company such as Carrier IQ—with which no end customer has any direct contact—can log customer activity on mobile devices down to the keystroke for later analysis without the knowledge of the user. Primary websites may pass information to affiliated companies, sell information to data aggregators and data exchanges directly, or allow a tracking company to place an invisible beacon or web bug on their website.

Table 1. Problems with tracking online by role.

Role	Problem	Key actors	Responsible because…	Suggested ethical actions
Supply chain	Potential harm from secondary use of information along the supply chain.	Primary website acting as a gatekeeper to the information supply chain.	Primary website benefit from harm caused to individuals within the information supply chain. Without primary website, individual would not disclose information. Relationship with individual acts as a lure for the individual to visit the site and disclose information.	Reveal tracking allowed on primary website or application.
	Possible breaching of privacy expectations and confidentiality in passing information within the supply chain.		Primary website has unique knowledge and ability to identify and stop tracking.	Set policies as to who has access to user data and for what purpose. Limit who has access.
Surveillance	Inability to *avoid* watcher.	Data aggregators with no direct relationship with users.	Residual harm from data aggregation—tracking actors benefit from the personality and identity of others while contributing to the harm of surveillance.	Keep data within functional silos so that no single actor has broad user data. Deidentify user information.
	Inability to *identify* watchers		Tactics by which data is collected are	Make watchers visible by

Companies collecting, aggregating, and disclosing consumer data are not homogeneous and take different strategic positions within the online space. At times, firms online are quickly categorized as either click-and-mortar sites, whose business is delivering products and services directly to consumers, or large tracking companies, which anonymously collect consumer data. However, firms differentiate using two mechanisms as illustrated in Figure 1: by the type of relationship held with the user (Bedi 2013; Ohm 2009) and by the type of information tracked and collected (Kerr 2009). Each axis and category is explored in the following.

Type of consumer relationship

Firms online vary based on the proximity of the firm to the end user. For instance, Sears.com's primary business is selling products and services to the end customer with whom it has a relationship, whereas Rapleaf is a data aggregator that can target down to a specific individual while remaining unknown to the majority of users (Steel 2010). Data aggregators remain in the background without a relationship with users while compiling individual profiles based on online activity with increasing resilience and intrusiveness (Tene and Polonetsky 2012); primary websites deal directly with the consumer to deliver products or services.

Yet the distinction between actors focused on front-end relationships and those focused on back-end processing is not always clear, as an actor may have a more complicated relationship with the user, as depicted in Figure 1. In "The Privacy Merchants," Amitai Etzioni (2012) highlights the growing threat to privacy by online firms and categorizes online actors into two types: firms that track consumers as a by-product of their primary business, versus firms that track consumers as their main line of business. For Facebook, much of its business model relies upon its back-end processing and commercial transactions rather than its front-end interface with Facebook users: a strategic choice blurring the line between a business that relies on a relationship with a user and a business that focuses on data retention and analysis for third parties (Stalder 2008). At a certain point, the business model of a firm suggests that information collection and aggregation are more important than the product or service seen by the users. Where Mastercard and Visa once only dealt with merchants, these firms have since become more consumer focused and have recently returned to a focus on back-end processing by possibly selling aggregated purchasing information to third parties (Steel 2011a, 2011b). Similarly, credit bureaus were once unknown to individuals and focused on being back-end processors of information before shifting to being more focused on the consumer relationship—with a different set of obligations. A firm's

relationship, therefore, can be framed along a continuum from customer facing to back-end processing that may change over time.

Breadth of information collected

Separately, firms decide to collect, store, and distribute different types of information. While special content and personalized information garners much attention, the type of content is not always useful in distinguishing sensitive information worthy of extraordinary protection. For example, information with clearly medical and financial details may be protected with additional regulations, but many inferences are possible from seemingly benign or innocent facts: When one searches for depression on dictionary.com, one is tracked using 223 tracking cookies (Etzioni 2012). The designations of sensitive, private, and personally identifiable categories are highly contextual (Nissenbaum 2009; Hartzog 2012; Schwartz and Solove 2011; Poritz 2007; Ohm 2009) and change over time.

Rather than information being specifically labeled as sensitive, as with financial or medical records, the breadth of information collected can be seen as contributing to the degree to which information gathered is considered personally identifiable or sensitive. The breadth of information can be based on the greater variety of information across contexts for a user or the greater volume of information aggregated over time—or both. For example, companies developed software to match pseudonyms and e-mail addresses, rendering previously anonymous information personally identifiable by combining data sets (Pariser 2011). Similarly, many firms regularly claim that no names are collected online, but RapLeaf identifies records by name and connects data to voter registration files, shopping histories, social networking activities, and real estate records by aggregating across many sources. Research is consistently identifying new ways to personally identify aggregated information

Google, and Facebook—broaden their services to oversee a broad array of consumer activities. Such Web portals (I) remain customer facing but gather, aggregate, and retain information across many contexts.

Roles and responsibilities of tracking online

When a firm makes a strategic choice online—and is situated in the matrix in Figure 1 above—that firm changes how privacy interests are respected by influencing what consumer information is seen by which actors and how the information is used and stored. Based on the information gathered and the type of relationship with users online in Figure 1, firms take on larger (or smaller) roles within three possible systems: as part of a supply chain of information, as a member of a system of surveillance, or as an arm of law enforcement. This exercise is similar to Akrich's (2000) and Latour's (2000) work in actor-network theory and Bijker's (1995) work within socio-technical systems, where a larger system of actors is considered in order to understand the roles and responsibilities of each individual actor. Importantly, and as shown in the following, a firm can take on a role within more than one system. Table 1 summarizes the roles and obligations of key actors based on their strategic position in Figure 1 and as explored here. For each role, I identify possible problems, key actors, and associated obligations of firms online.

As a member of a supply chain

In the typical offline business model, managing a supply chain has strategic and ethical implications: Software companies must ensure that their products are not eventually sold in Syria through a distribution center in Dubai; Apple is held accountable for the working conditions of their suppliers such as FoxConn (Horwitz and Asokan 2011; Duhigg and Barboza 2012). Similarly, online con-

Brunton and Nissenbaum (2011) note that daily online activities are regularly tracked,

> where every click and page may be logged and analyzed, explicitly providing data to the organizations on whose systems we interact. This data can be repackaged and sold, collected and sorted and acquired by a variety of means, and re-used for purposes of which we, the monitored, know nothing, much less endorse.

This passing of information from one actor to the next is prevalent online. A recent study found that out of the top 100 sites online, 85 had third-party cookies, 21 sites contained more than 100 cookies, and 11 sites contained more than 150 tracking cookies (Hoofnagle and Good 2012). In addition, websites are increasingly using persistent tracking mechanisms such as flash cookies and respawning devices that are impervious to user detection and deletion (Ayenson et al. 2011; Loftus 2011b).

Problems in the information supply chain

Two possible problems emerge within the information supply chain of online tracking that may be a concern to firms online: (1) Passing information may eventually be used with negative consequences to individuals or online communities, and (2) passing information may violate privacy norms as understood by users.

First, selling information to third parties may lead to an increased risk of secondary use or information leakage with eventual harm to users (Mayer and Mitchell 2012). Information may be used to modify insurance premiums or mortgage rates (Tene and Polonetsky 2012), to identify trends in demographics such as flu outbreaks, or to prioritize search results for a travel site (Mattioli 2012). Likewise, teens may receive targeted advertising for weight loss programs or depression medicine, which may further exacerbate teen angst (Angwin 2010). As such, the sensitivity of the information passed on to third parties in the supply chain is more a function of the type website, has a distinct set of associated privacy expectations based on the individual's relationship with the website and the context of the interaction. Individuals may expect location information to be used to offer hotel or restaurant discounts for their destination, but individuals do not expect that information be passed to data aggregators, stored for a year, and later used to make pricing decisions. Users disclose information with a purpose in mind and with an implicit social contract (Heeney 2012) or confidentiality agreement. Privacy law scholar Woodrow Hartzog (2012) suggests that this confidentiality agreement should be imposed on subsequent actors who receive or gather the information within a concept of "chain link confidentiality". The expectations present upon initial disclosure—who should receive information, how information can be used, how long information will be stored—should pertain throughout the information supply chain online.[2]

Obligations within the information supply chain. Firms with direct relationships to the user, such as online storefronts and Web portals in Figure 1, are in a unique position as gatekeepers between consumers and the many tracking companies within the supply chain. In effect, primary websites—those first-order actors with a direct relationship with the consumer—are necessary to the system of information tracking online: Without a relationship with the primary website, the user would not disclose information online. Within this role of gatekeeper, primary websites have a greater obligation based on their (1) relationship with the user and (2) unique knowledge and power in the online context.

First, the primary website or application has an additional responsibility to respect the privacy expectations of the user when that primary website decided to enter into the beneficial relationship with the individual. Primary websites have an obligation to understand and respect the privacy expectations around possible second-

The consumer relied upon this agreement when disclosing information, and the website has an obligation to uphold the agreement. In effect, the consumer's trust in the website to uphold the confidentiality agreement provides a lure to disclose information—if the user did not trust the website, presumably the user would not have visited the website and disclosed his or her information (McCole, Ramsey, and Williams 2010; Morgan-Thomas and Veloutsou 2013; Hoffman, Novak, and Peralta 1999). In breaching the confidentiality agreement, the website would be abusing the trust of the user.

Second, the primary website has unique knowledge to effectively limit the scope and type of consumer tracking. Primary websites make decisions as to which actors receive consumer information or which actors are allowed to track users on their website; the position of primary websites affords them the opportunity to enact change by modifying who is able to track users' information. Consumers, on the other hand, are not as fortunate. Studies show that rather than helping consumers, the tools to detect online tracking were more likely to cause confusion and, at times, accomplish the opposite of what the user intended (Leon et al. 2010). These flash cookies uniquely and persistently track even where individuals have "taken reasonable steps to avoid online profiling" (Ayenson et al. 2011; see also Loftus 2011c). As noted by privacy law scholars Rubenstein and Good (2012), websites must consider the vulnerability or sophistication of users when making privacy design decisions. Primary websites have an associated responsibility with unique knowledge and power within the supply chain to enact changes to the scope and type of tracking.

Individuals disclosing information to websites take on the risk "endemic in any relationship" of future disclosure (Bedi 2013). Although this is true, primary websites also take on the responsibility of the gatekeeper of a supply chain of information exchanges with a unique relationship with the consumer, position in the system, and

seen both as the institutionalized intrusion to privacy (Schwartz 1968) and as an issue distinct from privacy with unique implications to individuals and society (Regan 2011; see also Bennett 2011; Cohen 2008). Foucault used the architecture of hospitals and prisons as classic illustrations of surveillance, where persistent observation is used to maintain control (Foucault 1977; Bentham 1791). Foucault's panopticon includes a centralized, hidden actor in a tall guard tower to watch prisoners in surrounding prison cells (see also Bentham 1791). Importantly for actors online, Jeffery Rosen (2000) frames surveillance as the unwanted gaze from both direct observations as well as from searches on stored records, since the chilling effects on behavior are similar.

Problems in the system of surveillance

Surveillance takes away the ability of consumers to discriminately share information and to limit who receives what information and the purpose for which it is gathered. In general, surveillance contradicts the need of individuals to be unobserved (Benn 1984), as well as the need for uniqueness and a sense of self (Fried 1970; Rachels 1975; Bloustein 1964). An individual's personal space permits "unconstrained, unobserved physical and intellectual movement" for critical, playful subjectivity to develop as an individual and to cultivate relationships (Cohen 2008, p. 195). Importantly, "spaces exposed by surveillance function differently than spaces that are not so exposed" (Cohen 2008, 194), by changing how individuals behave and think due to the fear of being watched and judged by others.

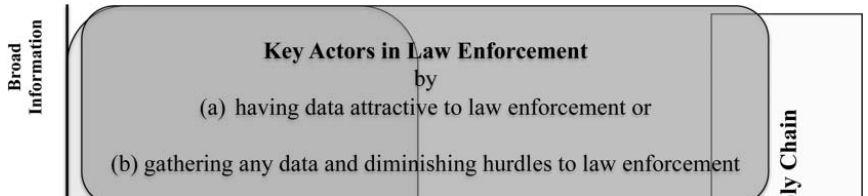
This need for a protected space extends online. Practically, consumers' online life is as deeply integrated into their social life and as radically heterogeneous as their offline life (Nissenbaum 2011). In fact, Strandburg (2011) makes the strong case that the online space acts as an extension of the home. Where the home was once

identify the watchers (Cohen 2008). In other words, both the breadth of information gathered and the tactic of invisibility contribute to the problem of surveillance online.

First, aggregating data across disparate contexts online contributes to the perception that surveillance is impossible to avoid yet also creates a data record that tells a richer, more personalized story than the individual data points. The Mosaic Theory of privacy explains why privacy scholars are concerned with all elements of tracking, including transaction surveillance and purchasing behavior (Strandburg 2011). The Mosaic Theory of privacy suggests that the whole of one's movements reveals far more than the individual movements it comprises (*United States v. Jones* 2012, D.C. Circuit, 647; Kerr 2012), where the aggregation of small movements across contexts is a difference in kind and not in degree (Strandburg 2011). As Brunton and Nissenbaum (2011) note, "Innocuous traces of everyday life submitted to sophisticated analytics tools developed for commerce and governance can become the keys for stitching disparate databases together into unprecedented new wholes" (online).

By aggregating across contexts and storing transaction data at the level of the individual, firms can create highly individualized products without a proportionate benefit to the user. Broad data aggregators summarize information across diverse contexts into profiles and sell aggregated information to companies looking for a specific, target market. Individualized aggregation is a strategic choice to create value for the firms and their eventual customer. Data aggregators increase the value of their product or service as more data are collected at a finer level of analysis. When data aggregators market their service as selling information about individuals, and not just groups of individuals based on demographics or geographic areas of interest, these firms use individuals' personas as their value proposition, rather than merely consolidated or obscured data. As such, firms such as data aggregators face the potential to use the individuals as a mere means with an increased harm of surveillance.

Second, most data aggregators are invisible to the user and thereby exacerbate the surveillance problem by being both unknown and unreachable. Unknown and invisible actors gathering and storing data contribute to the perception of omnipresent and omniscient surveillance. Remaining invisible while maintaining such an important role in a system of surveillance deceives the user and breaches minimal procedural social contract norms by not announcing the contractors' entrance (e.g., Donaldson and Dunfee 1994). In other words, as an actor with a disproportionate influence on whether or how privacy expectations are respected or undermined, broad tracking firms have an obligation to announce their presence in order to allow other contractors in the community (users) to further develop privacy expectations or exit the community by leaving the website. Privacy law scholar Bedi notes that third-party actors need not be an



active member of the relationships with users to have responsibilities (Bedi 2013, 62): "Why then should an individual user bear the burden of this additional risk, when the [third-party] server (the source of risk) makes no substantive contribution to the relationship."

The surveillance system online suggests the back-end processors in Figure 2—unknown to individuals yet aggregating data—have a special role in the surveillance system online as they are invisible to users while aggregating data across diverse sources. This need not be the case: Companies such as Intel, DuPont StainGuard, and Vibram soles (on minimalist running shoes) make the strategic choice to take a hidden portion of the consumers' product and ensure the end user is aware of its presence; similarly, hidden trackers of consumer data can make their presence known to the end user. Firms can lessen their role in consumer surveillance by becoming more visible to the consumers and keeping data within functional silos or within a particular context.

As an arm of law enforcement

Finally, in addition to acting within an information supply chain and as a part of a system of surveillance, online firms may play a role in law enforcement in the United States and globally. Law enforcement can use data tracked and gathered online by private firms for investigations and prosecutions. For example, in the second half of 2014, the U.S. government made 12,539 requests to Google for user data, and Google complied with some or all of the requested information 84% of the time (Google 2014). Twitter received 2,058 requests for information regarding 3,131 accounts, and of these requests, 1,257 were from the U.S. government; Twitter complied 72% of the time (Twitter 2014). More generally, Etzioni (2012) examines the role of private firms in law enforcement in "The Privacy Merchants" and notes that the U.S. government and law enforcement, such as the FBI, Main scenario. This concept is known in law as the third-party doctrine, where the presence of a third party to a transaction or activity eliminates any expectation of legal privacy. Kerr, a privacy law scholar, summarizes the third-party doctrine: "By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed. … In other words, a person cannot have a *reasonable expectation of privacy* in information disclosed to a third party" (Kerr 2009, 563, emphasis added). In law, this reasonable-expectations-of-privacy test is used to determine whether Fourth Amendment protections apply to the situation and, therefore, whether law enforcement must obtain a search warrant. In other words, the third-party doctrine is a hurdle to Fourth Amendment protections—an individual does not have a reasonable expectation of privacy to any communication he or she voluntary discloses to a third person (Bedi 2013).

Importantly for firms tracking users online, law enforcement can ask for consumer data without a warrant—and the associated high burden of proof and judge's signature required of a warrant—if an individual has no reasonable expectations of privacy. Online firms relinquish data without a warrant frequently. For example, of the 815 requests on Twitter user data from U.S. law enforcement in the second half of 2012, 60% had subpoenas, 11% had court orders, and only 19% had search warrants (Twitter 2014). Further, most requests remain hidden from the targets: Only 24% of requests resulted in user notification. U.S. law enforcement issues national security letters (NSLs) to compel firms, such as Internet service providers (ISPs), banks, credit bureaus, or Google, that have gathered and stored broad data of a users' activities, not only to disclose user data but also to remain quiet about the existence of a national security letter. In 2011, the FBI issued 16,511 NSLs on 7,201 different individuals (Kravets 2013a).

consumer information. If private firms benefit from storing data that are attractive to law enforcement and, in doing so, lower the hurdles to law enforcement accessing that data, the private firm should reconstitute the structures respecting private interests through policies around obscurity and disclosure. As noted by privacy law scholar Bedi, "a third party server may have its own rules (as Facebook does) that could curtail the government from freely acquiring the information" (Bedi 2013, 3 fn 14).

Firms gathering and storing information have a responsibility to reconstitute structures diminished by their actions by making obscurity an option for consumers. Obfuscation techniques can be offered for consumers, whereby noise is added to the stored data to make collection more ambiguous, confusing, harder to use, and less valuable (Brunton and Nissenbaum 2011). Obscurity can be a factor in determining "plain view" and degree of "public"—when users attempt to hide or obscure their data, courts may decide that the information deserves more protection (Hartzog and Stutzman 2013). In addition, separate, nonlinked databases, encryption, limited sharing, and deidentification are all techniques to obscure the data for consumers (Martin 2013). Law enforcement can be asked to use warrants with probable cause to gain access to some online information held by private actors (Kravets 2013b).

However, the mere presence of the firm may change the reasonable expectations of privacy tests within the law based on the third-party doctrine. Individuals can only take affirmative steps to change their disclosure decisions if aware of the presence of third parties and the potential access of law enforcement. Opportunities to recognize the existence of third parties do exist: Browser add-ons such as Ghostery (www.ghostery.com) allow users to easily identify the tracking companies on a primary website and block those companies. Either browsers or primary websites should develop a mechanism to show the mere presence of tracking companies on the

of a certain thickness, understood norms, and industry regulations at the time of the disclosure. Individuals disclose information with an expectation of who can see it and how hard it is to access at the time of disclosure. However, when disclosure is disassociated with surveillance, as is the case when data is stored, the known technical capabilities, sophistication of other users, and possible risks with disclosure evolve in the intervening months or years. Firms storing information online leave individuals vulnerable to the problem where information disclosed that seems difficult to access by others—including law enforcement—is suddenly readily available based on new technological abilities. These firms can also delete information to make the data less attractive to law enforcement and to close the temporal gap between an individual disclosing data and law enforcement accessing data.

Discussion and conclusion

This article focused on the roles and responsibilities of online tracking companies such as data aggregators and ad networks, as well as primary websites such as Web portals and online storefronts. Firms' roles and responsibilities in tracking users online depend on the strategic choices of firms about their relationship with users and the type of information gathered. Table 1 summarizes the problems with tracking online, the associated key actors, and the responsibilities of firms tracking and aggregating online. Additional work within information studies, science and technology studies, and business ethics could compare current practices of actors online to the suggested obligations and recommend better practices to bridge the gap between current actions and responsible goals.

The ubiquity of big data in the private sector has led to widespread use of a complicated system of tracking and big data without an understanding of the firm's

storage and access of user information, with a unique relationship with the user, position in the system, and requisite knowledge to enact change. Such primary websites should develop policies as to which actors are granted access to their consumers' data and make those actors known to the user at all times. Privacy or data impact assessments are one step in this direction by placing an obligation on firms to understand their role in data management and privacy (Wright 2013). Similar to the manner in which Wal-Mart is held accountable for the norms and behavior within its supply chain, and BlueCoat is held accountable for how its software is used within their supply chain, primary websites and applications should be held accountable for how their supply chain utilizes their users' information. More work could be done extending the examination of supply chains and responsibility offline to the existence of supply chains of information online.

Broad, pervasive, and persistent trackers online are key players within a larger system of surveillance online by contributing to users not being able to identify who is watching them and not being able to escape the watchers. By becoming more visible and keeping data within distinct functional contests—such as Datium, which aggregates only within automotive sales—tracking firms could minimize their role in this surveillance. More work could be done within business ethics by empirically examining the degree to which individuals are tracked online and the degree to which individuals are knowledgeable of that surveillance. For example, the option of a "home mode" on a mobile device (Popescu and Baruh 2013) would simulate the sanctity of the home if respected by data aggregators and trackers.

Finally, while much has been commented on about Internet companies operating globally and about foreign law enforcement coercing U.S. Internet companies to provide information, 81% of all information requests for Twitter came from U.S. law enforcement (Twitter 2014). mobile apps (Shilton and Martin 2013) and online (Martin, 2015) and as further explored in note 2. More work is needed to continue to identify to privacy expectations of consumers so that firms are able to fulfill their responsibilities and create a sustainable online experience that creates value through operational efficiency and product development and that respects expectations of consumers. In particular, work that attempts to both leverage the benefits of big data and respect privacy expectations through engineering, such as Mayer and Narayanan (2013), would offer firms a path forward.

Alternatively, the act of sharing information is sometimes mistakenly framed as dispositive of relinquishing an expectation of privacy: Individuals either share information and lose a right to privacy, or do not share information and retain a reasonable expectation of privacy. As such, individuals are incorrectly assumed to give up a large measure of privacy when we enter the public sphere (e.g., Alfino and Mayes 2003). For example, Sun Microsystems chief executive Scott McNealy famously said in 1999, "You have zero privacy anyway … Get over it" (Sprenger 1999). And in 2012, Google Chief Executive Eric Schmidt stated, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Popkin 2010, online). This alternative places no responsibility on firms to respect privacy expectations, since privacy expectations are (mistakenly) assumed to not exist.

In examining the roles of the many firms online tracking users, this article is a first step to identify the responsibilities of actors in tracking, gathering, storing, and disclosing user data. This article suggests that if a firm wishes to uphold its obligations online, that firm will need to decrease its roles within a supply chain of information, in a system of surveillance, and as an arm of law enforcement. Such firms benefit from aggregating and analyzing user data and have an associated responsibility to minimize the harm to users and enact change where they are

2. For example, research has shown users have privacy expectations around both the type of information accessed and how the information is used when using mobile apps (Shilton and Martin 2013) or when online (Martin 2015). Respondents care about the scope of use of even innocuous information online (Leon et al. 2013), view tracking and online behavioral advertising as creepy (Ur et al. 2012), and wish to not be tracked (McDonald and Cranor 2010). In addition, respondents are concerned when notified by the researcher about the degree to which the individuals are tracked (Wills and Zeljkovic 2011). When asked, 68% of respondents stated they would not allow tracking (Turow et al. 2009).

Acknowledgments

I thank Katie Shilton and Mary Culnan for helpful comments on an earlier draft of this article. This article was presented to the Society of Business Ethics (2013).

Funding

This material is based upon work supported by National Science Foundation grant 1311823—Addressing Privacy Online.

References

Akrich, M. 2000. The de-scription of technical objects, In *Shaping technology/building society: Studies in sociotechnical change*, ed. W. Bijker and J. Law, 205–24. Cambridge, MA: MIT Press.

Alfino, M., and G. R. Mayes. 2003. Reconstructing the right to privacy. *Social Theory and Practice* 29 (1):1–18.

Angwin, J. 2010. The Web's new gold mine: Your secrets. *Wall Street Journal*, July 10. http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404 (accessed May 3, 2015).

Ayenson, M., D. Wambach, A. Soltani, N. Good, and C. Hoofnagle. 2011. Flash cookies and privacy II: Now with HTML5 and etag respawning. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390 (accessed September 24, 2015).

Bijker, W. 1995. *Of bicycles, Bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge, MA: MIT Press.

Bloustein, E. 1964. Privacy as an aspect of human dignity: An answer to Dean Proseer. *New York University Law Review* 39:962–1007.

Boyd, D., and K. Crawford. 2012. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication, & Society* 15 (5):662–79.

Brunton, F., and H. Nissenbaum. 2011. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday* 16 (5): online. http://firstmonday.org/article/view/3493/2955 (accessed May 3, 2015).

Buitelaar, J. 2014. Privacy and narrativity in the Internet era. *The Information Society* 30 (4):266–81.

Calo, R. 2012. Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review* 87:1027–72.

Calo, R. 2013. Consumer subject review boards: A thought experiment. *Stanford Law Review* 66:97.

Cohen, J. 2008. Privacy, visibility, transparency, and exposure. *University of Chicago Law Review* 75 (1):181–201.

Cranor, L. F., C. Hoke, P. G. Leon, and A. Au. 2014. Are they worth reading? An in-depth analysis of online advertising companies' privacy policies. Presented at 42nd Research Conference on Communication, Information and Internet Policy (TPRC 2014), March 31. https://www.andrew.cmu.edu/user/pgl/tprc2014.pdf.

Donaldson, T., and T. Dunfee. 1994. Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review* 19 (2):252–84.

Duhigg, C., and D. Barboza. 2012. In China, human costs are built into an iPad. *The New York Times*, January 25. http://www.nytimes.com/2012/01/26/business/ieconomy-apples-ipad-and-the-human-costs-for-workers-in-china.html?pagewanted=all (accessed September 24, 2014).

Etzioni, A. 2012. The privacy merchants: What is to be done? *University of Pennsylvania Journal of Constitutional Law* 14 (4):929.

Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: Recommendations for business and policymakers. March. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (accessed May 3, 2015).

Hoofnagle, C., and N. Good. 2012. *The Web privacy census*, October. http://law.berkelet.edu/privacycensus.htm. (accessed September 24, 2014).

Horwitz, S., and S. Asokan. 2011. U.S. probes use of surveillance technology in Syria. *The Washington Post*, November 18. http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQAS1iEVN_story.html (accessed September 24, 2014).

Kerr, O. 2009. The case for the third-party doctrine. *Michigan Law Review* 107:951 (accessed 9/24/2014).

Kerr, O. 2012. The mosaic theory of the Fourth Amendment. *Michigan Law Review* 111 (3):311–54.

Kravets, D. 2013a. Alleged drug dealer at center of Supreme Court GPS case wins mistrial. *Wired*, March 4. http://www.wired.com/2013/03/gps-drug-dealer-retrial/ (accessed September 24, 2014).

Kravets, D. 2013b. Google says the FBI is secretly spying on some of its customers. *Wired*, March 5. http://www.wired.com/2013/03/google-nsl-range (accessed 9/24/2014).

Laney, D. 2001. 3D data management: Controlling data volume, velocity, and variety. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. (accessed September 24, 2014).

Langenderfer, J., and D. Cook. 2004. Oh, what a tangled web we weave: The state of privacy protection in the information econ**o**my and recommendations for governance. *Journal of Business Research* 57 (7):734–47.

Latour, L. 2000. Where are the missing masses? The sociology of a few mundane artifacts. In *Shaping technology/building societies: Studies in socio-technical change*, ed. W. Bijker and J. Law, 225–28. Cambridge, MA: MIT Press.

Leon, P. G., L. F. Cranor, A. M. McDonald, and R. McGuire. 2010. Token attempt: The misrepresentation of website privacy policies through the misuse of p3p compact policy tokens. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society* (pp. 93–104). New York, NY: ACM.

Leon, P. G., J. Cranshaw, L. F. Cranor, J. Graves, M. Hastak, B. Ur, and G. Xu. 2012, October. What do online behavioral advertising privacy disclosures communicate to users?. In *Proceedings of the 2012 ACM workshop on Privacy in the electronic society* (pp. 19–30). New York, NY: ACM.

Loftus, T. 2011b. FTC settles with online advertiser over flash cookie use. *Wall Street Journal*, November 8. http://blogs.wsj.com/digits/2011/11/08/ftc-settles-with-online-advertiser-over-flash-cookie-use/ (accessed September 24, 2014).

Loftus, T. 2011c. Study: Usability issues plague tools that limit online behavioral advertising. *Wall Street Journal*, October 31. http://blogs.wsj.com/digits/2011/10/31/study-usability-issues-plague-tools-that-limit-online-behavioral-advertising/ (accessed September 24, 2014).

Lohr, S. 2012. How big data became so big. *The New York Times*, August 11. http://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html?pagewanted = all&_r = 0 (accessed September 24, 2014).

Martin, K. E. 2012a. Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics* 111 (4):1–21.

Martin, K. 2012b. Information technology and privacy: Conceptual muddles or privacy vacuums? *Ethics and Information Technology* 14 (4):267–84.

Martin, K. 2013. Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday* 18 (12): Online. http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 (accessed May 3, 2015).

Martin, K. 2015. Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing* 34 (2):210–27.

Mattioli, D. 2012. How Orbitz targets its site's visitors. *Wall Street Journal*, June 25. http://blogs.wsj.com/digits/2012/06/25/how-orbitz-targets-its-sites-visitors (accessed September 24, 2014).

Mayer, J., and J. Mitchell. 2012. Third-party web tracking: Policy and technology. In *Proceedings of the 2012 IEEE symposium of security and privacy*, 413–27. Washington, DC: IEEE Computer Society.

Mayer, J., and A. Narayanan. 2013. Privacy substitutes. *Stanford Law Review Online* 66:89. http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-substitutes (accessed May 3, 2015).

McDonald, A. M., and L. F. Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4:543–97.

McDonald, A., and L. F. Cranor. 2010. Beliefs and behaviors: Internet users' understanding of behavioral advertising.

Nissenbaum, H. 2011. A contextual approach to privacy online. *Daedalus* 140 (4):32–48.

Ohm, P. 2009a. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57:1701.

Ohm, P. 2009b. The rise and fall of invasive ISP surveillance. *University of Illinois Law Review* 1417–96.

Ohm, P. 2015. Sensitive information. *Southern California Law Review* 88.

Pariser, E. 2011. What the Internet knows about you. *CNN*, May 22. http://www.cnn.com/2011/OPINION/05/22/pariser.filter.bubble/ (accessed September 24, 2014).

Popescu, M., and L. Baruh. 2013. Captive but mobile: Privacy concerns and remedies for the mobile environment. *The Information Society* 29 (5):272–86.

Popkin, H. 2010. Privacy is dead on Facebook. Get over it. *NBC News*, January 13. http://www.nbcnews.com/id/34825225/ns/technology_and_science-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.U-DTKPldU5E (accessed September 24, 2014).

Poritz, J. A. 2007. Who searches the searchers? Community privacy in the age of monolithic search engines. *The Information Society* 23 (5):383–89.

Rachels, J. 1975. Why privacy is important. *Philosophy and Public Affairs* 4:323–33.

Regan, P. 2011. Response to Bennett: Also in defense of privacy. *Surveillance and Society* 8 (4):497–99.

Rosen, J. 2000. *The unwanted gaze: The destruction of privacy in America*. New York, NY: Random House.

Rubenstein, I., and N. Good. 2012. *Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents (Public Law Research Paper No. 12-43)*. New York, NY: New York University School of Law.

Schwartz, B. 1968. The social psychology of privacy. *American Journal of Sociology* 73 (6):741–852.

Schwartz, P., and D. Solove. 2011. The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review* 86:1814.

Shilton, K., and K. E., Martin, Mobile Privacy Expectations in Context. 2013. Paper presented at TPRC 41: The 41st research conference on communication, information and Internet policy, Arlington, VA, September 27–29. http://dx.doi.org/10.2139/ssrn.2238707 (accessed September 20, 2015).

Sloan, R., and R. Warner. 2014. Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law*

Stalder, F. 2008. Bourgeois anarchism and authoritarian democracies. *First Monday* 13 (7): online. http://pear.accc.uic.edu/ojs/index.php/fm/article/viewArticle/2077 (accessed May 3, 2015).

Steel, E. 2010. A Web pioneer profiles users by name. *Wall Street Journal Digits*, October 25. http://online.wsj.com/news/articles/SB10001424052702304410504575560243259416072 (accessed September 24, 2014).

Steel, E. 2011a. MasterCard's talks with Madison Avenue. *Wall Street Journal*, October 24. http://blogs.wsj.com/digits/2011/10/24/mastercards-talks-with-madison-avenue (September 24, 2014).

Steel, E. 2011b. Visa's blueprint for targeted advertising. *Wall Street Journal*. October 24. http://blogs.wsj.com/digits/2011/10/24/visas-blueprint-for-targeted-advertising (September 24, 2014).

Strandburg, K. 2011. Home, home on the Web and other Fourth Amendment implications of technosocial change. *Maryland Law Review* 70:614–80.

Tene, O., and J. Polonetsky. 2012. Privacy in the age of big data: A time for big decisions. *Stanford Law Review* 64:63–69.

Tene, O., and J. Polonetsky. 2013. Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property* 11 (5): 240–73.

Turow, J., J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy. 2009. Americans reject tailored advertising and three activities that enable it. SSRN 1478214.

Twitter. 2014. Information requests: Transparency report. https://transparency.twitter.com/information-requests/2014/jan-jun (accessed November 21, 2015).

United States v. Jones. 2012. 615 F.3d 544 (D.C. Cir. 2010), aff'd sub nom. United States v. Jones, 132 S. Ct. 945. Sotomayor, J. concurring. http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf (accessed September 24, 2014).

Ur, B., P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang. 2012, July. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the eighth symposium on usable privacy and security,* 4. New York, NY: ACM.

U.S. Senate, Committee on Commerce, Science, and Transportation. 2013. A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes. http://www.commerce.senate.gov/public/?a = Files.Serve&File_id = 0d2b3542-6221-4888-a631-08f2f255b577