Data Aggregators, Consumer Data, and Responsibility Online:

Who is tracking consumers online and should they stop?[1]

Provisionally Accepted
The Information Society

Kirsten Martin, Ph.D.

George Washington University
School of Business

martink@gwu.edu

October 2014

Data Aggregators, Consumer Data, and Responsibility Online:

Who is tracking consumers online and should they stop?[2]

The goal of this paper 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.

KEYWORDS: Privacy, Internet, big data, business ethics, surveillance, tracking online.

INTRODUCTION

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 2013). 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 healthcare, mobile, smart grids, traffic management, retail, and payment services (Tene and Polonetsky 2013).

While recent advances have led to a democratization of big data, where more actors have access to more consumer information with better, faster, and cheaper tools, the tactics to address online privacy continue to languish (Langenderfer and Cook 2004). The Federal Trade Commission's reliance on Fair Information Practices (FIP), and notice and choice in particular, serves as a source of guidance for self-regulation within the industry (FTC 2012), yet considerable agreement exists that notice and choice has failed to govern privacy effectively online (Martin 2013; Nissenbaum 2011; Schwartz and Solove 2011; Calo 2012; Solove 2013).[3] Consumers fall victim to 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 summarize the idea behind notice and choice (2011): 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 the main responsibility of the firm, firms become free to implement questionable privacy practices so long as the practices are accurately reported. As more firms have access to consumer data, little prescriptive guidance is offered in developing strategies for consumer information.

While the policy focus has been on consumer choice and the associated user responsibility in disclosing information, this paper shifts the attention to the strategic choices of firms online and their associated responsibility in collecting, aggregating, storing, and sharing consumer information. The goal of this paper is to critically analyze the strategic choices of firms collecting 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' 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 paper proceeds as follows. First, I categorize firms online based on two important strategic decisions concerning a firm's relationship with consumers and 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.

Table 1: Problems with Tracking Online by Role

<table>
<tr><th>…</th><th>Problem</th><th>Key Actors</th><th>Responsible Because…</th><th>Suggested Ethical Actions</th></tr>
<tr><td rowspan="2">Supply Chain</td><td>Potential harm from secondary use of information along the supply chain.</td><td rowspan="2">Primary website acting as a gatekeeper to the information supply chain.</td><td>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.</td><td>Reveal tracking allowed on primary website or application.</td></tr>
<tr><td>Possible breaching of privacy expectations and confidentiality in passing information within the supply chain.</td><td>Primary website has unique knowledge and ability to identify and stop tracking.</td><td>Set policies as to who has access to user data and for what purpose. Limit who has access.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Surveillance</td><td>Inability to avoid watcher</td><td rowspan="2">Data aggregators with no direct relationship with users</td><td>Residual harm from data aggregation – tracking actors benefit from the personality and identity of others while contributing to the harm of surveillance.</td><td>Keep data within functional silos so that no single actor has broad user data.

De-identify user information.</td></tr>
<tr><td>Inability to identify watchers</td><td>Tactics by which data is collected is deceptive and disrespectful to individuals by not maintaining minimum social contract norms that require the ability to identify contractors (trackers) and give contractors (the individuals) a voice.</td><td>Make watchers visible by browser or primary website/application</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Law Enforcement</td><td>Storing data and leaving individual vulnerable to changing ability of law enforcement.</td><td rowspan="2">Actors who benefit from aggregated and individualized data render the data attractive to law enforcement</td><td>Retaining data makes the individual vulnerable. An already disadvantaged party online – the user – is made worse off in retaining data.</td><td>Add options to make data obscure or less personally identifiable.

Diminish size of dataset: delete data; collect less data.</td></tr>
<tr><td>Lowering hurdles for law enforcement to access information by making data more accessible</td><td>Actors online that change the structure of privacy expectations have a responsibility to fix what was broken.

By breaking an existing structure that was relied upon to uphold privacy interests online, the actors voluntarily take on the responsibility to reconstitute the social and technological structures.</td><td>Implement transparency reports (such as Google and Twitter).

Make presence visible to end users to allow users to make decisions about disclosure

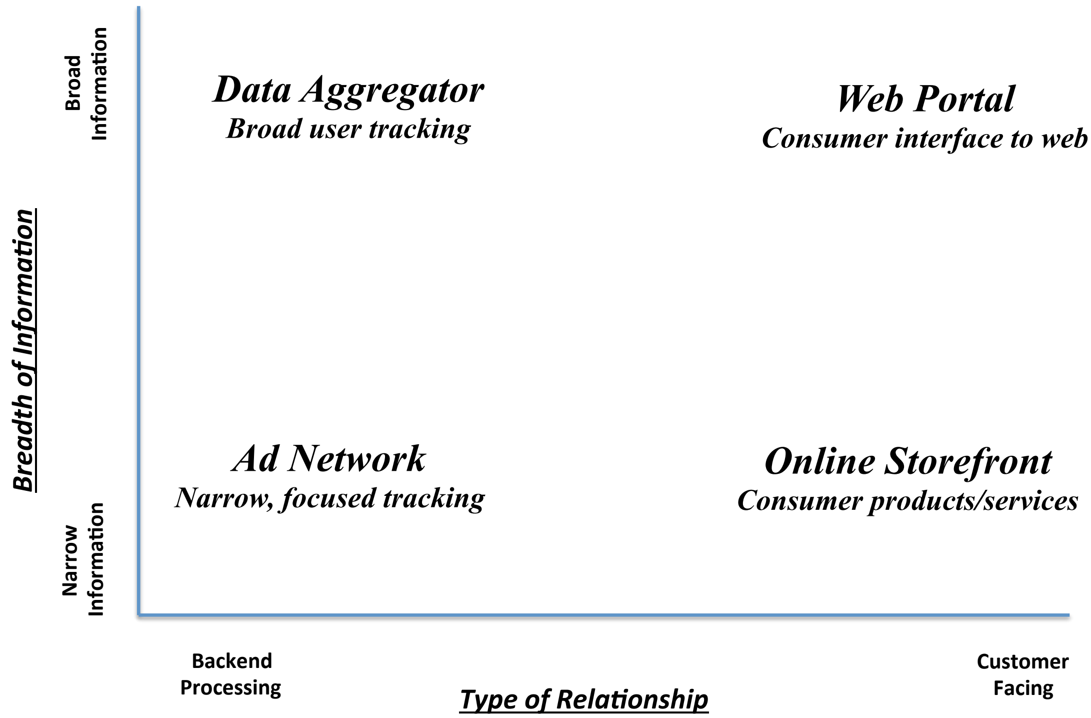
Have own policies as to when and why to disclose data to law enforcement.</td></tr>
</table>

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 whom no end customer has any direct contact – can log customer activity on mobile devices down to the key stroke for later analysis without the knowledge of the user (Loftus 2011a). 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.

Companies collecting, aggregating, and disclosing consumer data are not homogenous 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, who 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 below.

Figure 1:
Categorizing Actors Online by the Breadth of Information and Relationship with Users



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 they have 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 backend 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 their business model relies upon their backend processing and commercial transactions rather than their 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 is 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 backend processing by possibly selling aggregated purchasing information to third parties (Steel 2011). Similarly, credit bureaus were once unknown to individuals and focused on being backend 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 backend 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, the user 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 2010) 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 email 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 (Ohm, 2014).

In Figure 1, these two strategic choices – the relationship with the consumer and the breadth of information collected – combine to form four general types of tracking firms online. Data aggregators (II) gather and store consumer data across many contexts, such as RapLeaf and ChoicePoint who link information from multiple online sources into a behavioral profile and may add offline data as well. Ad networks (III) are similarly hidden from users providing a market place for advertisers to buy information in order to target ads and may limit the data collection to within a particular context or over a specific period of time. Within customer-facing firms (IV), online storefronts remain within a narrow context to serve customers while other firms – such as Amazon, 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 below, 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 consumer data might be passed from one firm to the next within an information supply chain, comparable to a traditional supply chain in the offline world. Within this supply chain narrative, consumers pass information to websites, who then pass the information to tracking companies, who may also pass the data to data aggregators. Data aggregators act as distributors online by holding consolidated information of many users across many contexts. When the user returns to browse or shop online, an ad network may utilize information from the data aggregator in order to place an advertisement on a website. A vertical supply chain is then created with multiple firms exchanging information and adding value to the data.

This information supply chain includes all types of data – no matter how small and seemingly innocuous. 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 over 100 cookies, and 11 sites contained over 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 2011).

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 of possible harm rather than a discrete category such as financial or medical information (Etzioni 2012). Work within targeted advertising and marketing ethics illustrates the range of harms from secondary use of tracked information (e.g., Moore and Rideout 2007). A broad range of information could be used with negative consequences.

Second, since information disclosed to a website is shared within a set of privacy rules, sharing information to new actors within the supply chain may breach the privacy expectations of consumers – regardless of any identified harm. In other words, information always has a 'terms of use' or norms governing when, how, why, and where it is to be used (Nissenbaum 2009; Martin 2012a). For example, information shared with Orbitz, a travel 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 suggests that this confidentiality agreement should be imposed on subsequent actors who receive or gather the information within a concept of "chain link confidentiality" (2012). 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.[4]

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 gatekeeper 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 secondary use of the information and to not deceive or use the individual. In other words, the primary website benefits from both the information and the relationship with the user and therefore has an assumed obligation not to use the information or the individual as a mere means to the firm's goals through deception or disregard for consumers' expectations. The more a firm benefits from individuals disclosing information, e.g., firms whose business model is dependent on sharing information such as social networking sites, take on a greater obligation to understand consumers' privacy expectations.

Within the user relationship, the primary website can be viewed as entering into an implicit confidentiality agreement governing who can access the information and how the information will be used (Hartzog 2012). The consumer relied upon this agreement when disclosing information and the website has an obligation to uphold the agreement. In effect, the consumers' 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 their 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. 2012; see also Loftus 2011). 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 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 knowledge to enact change. Similar to the manner in which Wal-Mart is held accountable for the norms and behavior within its supply chain, or BlueCoat is held accountable for how its network surveillance software is used by the Syrian government within their supply chain, primary websites and applications should be held accountable for how their information supply chain utilizes their users' information when they benefit from the disclosure of information and voluntarily remain in that position.

As A Member Of A Larger System Of Surveillance

Online firms may also take on a role within a larger system of surveillance online. Traditionally, surveillance is seen as both the institutionalized intrusion to privacy (Schwartz 1968) and as a distinct issue from privacy with unique implications to individuals and society (Regan 2011; see also Bennett 2011 and 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). 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 actor 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 individuals' 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, p. 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 seen as the physical demarcation of what information and behavior needs protecting from intrusion or surveillance, the home is no longer the primary storage facility for important documents, such as bank records, electrical bills, receipts, pictures, or protected conversations. Individuals retain an interest in controlling their identity and personal dignity online by managing the information that is shared (Buitelaar 2014).

Obligations Within the System of Surveillance

Firms who take part in pervasive, unseen surveillance have a responsibility for the problems created by their business model in Figure 1. Specifically, surveillance is particularly effective in changing behavior and thoughts when individuals (1) cannot avoid the gaze of the watcher and (2) cannot 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.

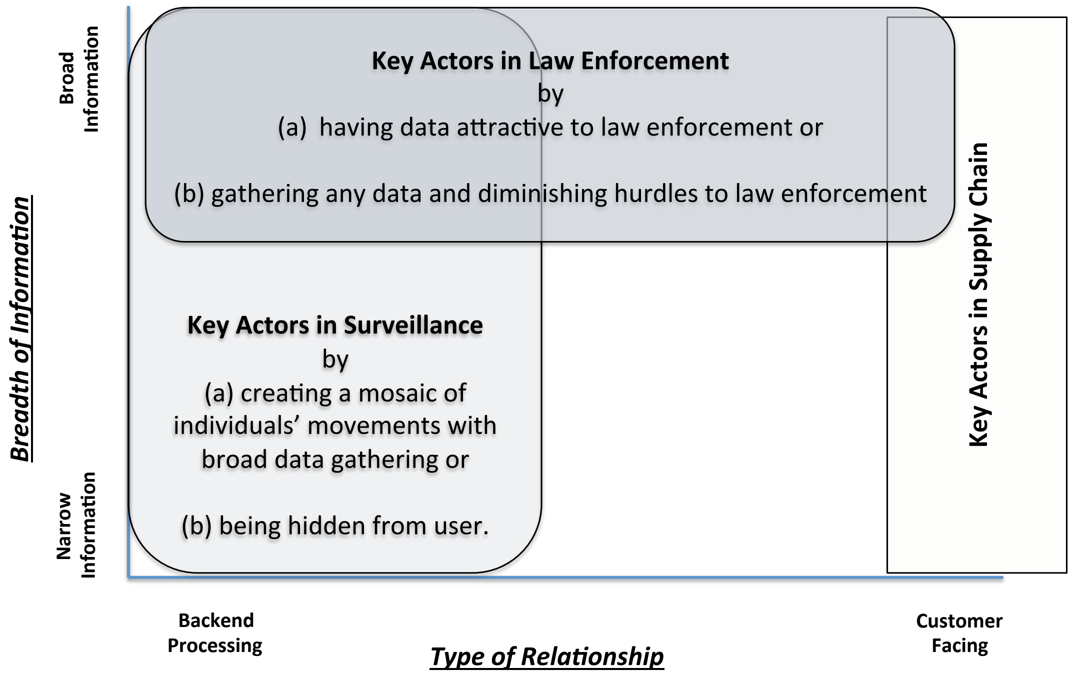
First, aggregating data across disparate contexts online contributes to the perception that surveillance is impossible to avoid yet also creates a data record that tells a richer, more personalized story than the individual data points. The Mosaic Theory of privacy explains why privacy scholars are concerned 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; DC Circuit, p. 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 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" (2011).

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 is 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): "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 backend 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.

Figure 2: Roles and Obligations Online By Type Of Online Tracking Actor.



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 2012, the U.S government made 8,438 requests to Google for user data, and Google complied with some or all of the requested information 88% of the time (Kelly 2013). Twitter received 1,858 requests for information regarding 1,433 accounts, 815 of which were from the U.S. government; Twitter complied 57 percent of the time (Miller 2013; Kelly 2013). 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 F.B.I., Main Department of Justice, U.S. Marshalls, D.E.A., I.N.S., and D.H.S., access consumer transaction data through data aggregators such as ChoicePoint and SeisInt and access phone records through companies such as AT&T, Verizon, and Bell South (see also Loftus 2012).

Problems as an Arm of Law Enforcement

These online records are attractive to law enforcement not only for the story that the transaction data can tell, but also because information gathered and stored by websites and tracking companies is no longer protected from law enforcement as it would be in an offline 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, *emphasis added*). In law, this reasonable-expectations-of-privacy test is used to determine if Fourth Amendment protections apply to the situation and, therefore, if 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 2013). Further, most requests remain hidden from the targets: only 24% of requests resulted in user notification. U.S. law enforcement issues national security letters (NSL) to compel firms, such as ISPs, banks, credit bureaus, or Google, who 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 2013b).

Obligations as an Arm of Law Enforcement

Online actors who aggregate data attractive to law enforcement take on two important roles within the law enforcement system by (1) changing the structure by which privacy is respected in becoming a 'third party' and (2) making the user more vulnerable to privacy violations by retaining data.

First, online actors change the structures upholding privacy interests online by collecting, aggregating, storing, and organizing information now easily accessible by law enforcement. Within this role as a 'third party', online firms change how privacy interests of individuals are recognized by lowering two hurdles existing in the offline world: the manpower required to consolidate information and the burden of proof required to collect consumer information. If private firms benefit from storing data that is 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).

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, non-linked databases, encryption, limited sharing, and de-identification 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 primary sites in order for individuals to make disclosure and obscurity decisions. Google was seen as a pioneer with their transparency report where Google (and now Twitter) disclose law enforcement's attempts to access user information. Both Google and Twitter are primary actors with a relationship with the user and have agreed to provide this data on law enforcement's access to their information. All actors who gather, store, and benefit from user data should **provide similar transparency reports** on law enforcement's activity with their data.

Finally, with extensive storing of individualized data attractive to law enforcement, online firms can make users more vulnerable to privacy violations online. Individuals disclose information *as if* a particular structure is in place; i.e., information disclosure is based on walls 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. We disclose more in a private room with close friends than in an open space with strangers close by. 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 paper 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 responsibilities for their role. Where academics, statisticians, and engineers must justify their data collection and analysis according to professional and institutional review board guidelines, "a private company that would conduct experiments involving thousands of consumers using the same basic techniques, facilities, and personnel faces no such obligations, even where the purpose is to profit at the expense of the research subject" (Calo 2013).

Specifically, actors online have a responsibility for their roles in multiple systems online**.** Primary websites and applications are partially responsible for the possible harm from secondary use of information within the information supply chain. Web portals and online storefronts are in a position of a gatekeeper to the subsequent 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 who 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 2013). Firms who create a dataset that is attractive to law enforcement or whose mere presence diminishes Fourth Amendment protections for users have an obligation to provide transparency reports and make their presence better understood by users. In addition, firms could understand their role within law enforcement by making their dataset less attractive by either obscuring the data or diminishing the size of the dataset (i.e. deleting data).

This paper relies on relies on the argument that individuals visit websites or applications while retaining expectations of privacy around the type of information collected and how the information is stored, used, and shared. For example, research has shown users have privacy expectations around both the type of information collected as well as how the information is used using mobile apps (Shilton and Martin 2013) and online (Martin, 2014) and as further explored in Note 3. 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.

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., Mayes and Alfino 2006). 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). The alternative places on responsibility on firms to respect privacy expectations since privacy expectations are assumed to not exist.

In examining the roles of the many firms online tracking users, this paper is a first step to identify the responsibilities of actors in tracking, gathering, storing, and disclosing user data. This paper suggests that if a firm wishes to uphold their obligations online, firms will need to decrease their roles within a supply chain of information, a system of surveillance, and as an arm of law enforcement. These 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 in the most knowledgeable and powerful position.

NOTES

[1] This material is based upon work supported by National Science Foundation grant #1311823 – Addressing Privacy Online. I wish to thank Katie Shilton and Mary Culnan for helpful comments on an earlier draft of this paper. This paper was presented at the American Statistical Association (2014), American Association of Public Opinion Researchers (2014), Philosophy of Management (2014), and Society of Business Ethics (2013).

[2] This material is based upon work supported by National Science Foundation grant #1311823 – Addressing Privacy Online. I wish to thank Katie Shilton and Mary Culnan for helpful comments on an earlier draft of this paper. This paper was presented at the American Statistical Association (2014), American Association of Public Opinion Researchers (2014), Philosophy of Management (2014), and Society of Business Ethics (2013).

[3] Empirical studies have also shown that notices are difficult if not impossible to find by users (Leon et al. 2012) and include false information (Leon et al. 2010). Respondents do not understand the notice to the point where users are misled by icons and notices (Ur et al. 2012). Respondents have been found to *assume* their privacy expectations are ncluded in the notice (Martin, 2014) or that the advertising icon does more to protect their privacy than in actuality (Leon et al. 2012). Notices are unrealistically time consumer (McDonald and Cranor 2008) and not always targeted towards consumers (Cranor et al. 2014).

[4] For example, research has shown users have privacy expectations around both the type of information access as well as how the information is used using mobile apps (Shilton and Martin 2013) or websites (Martin 2014) , care about the scope of use of even innocuous information online (Leon et al. 2013; Leon et al.), view tracking and online behavioral advertising as creepy (Ur et al. 2012), wish to not be tracked (McDonald and Cranor 2010). In addition, when individuals are notified by the researcher the degree to which they are tracked, respondents are concerned (Wills and Zeljkovic 2011). When asked, 68% of respondents stated they would not allow tracking (Turow et al. 2009).

Bentham, Jeremy. 1791. *Panopticon or the Inspection House*. Vol. 2.

———. "Panopticon (1787)." *Jeremy Bentham: The Panopticon Writings*.

Cranor, Lorrie Faith, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au. 2014. "Are They Worth Reading? An In-depth Analysis of Online Advertising Companies' Privacy Policies." *An In-Depth Analysis of Online Advertising Companies' Privacy Policies (March 31, 2014)*.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. Random House LLC.

Laney, Douglas. 2001. "3D Data Management: Controlling Data Volume, Velocity, and Variety." Gartner. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Leon, Pedro Giovanni, Lorrie Faith Cranor, Aleecia M McDonald, and Robert McGuire. 2010. "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of p3p Compact Policy Tokens." In , 93–104. ACM.

Leon, Pedro Giovanni, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. "What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?" In , 19–30. ACM.

Leon, Pedro Giovanni, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh. "Why People Are (Un) Willing to Share Information with Online Advertisers."

Leon, Pedro Giovanni, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. "What Matters to Users?: Factors That Affect Users' Willingness to Share Information with Online Advertisers." In , 7. ACM.

McDonald, Aleecia M, and Lorrie Faith Cranor. 2008. "Cost of Reading Privacy Policies, the." *ISJLP* 4: 543.

———. 2010. "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising." In .

Shilton, Katie, and Kirsten E Martin. 2013. "Mobile Privacy Expectations in Context." In . TPRC.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." *Available at SSRN 1478214*.

Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising." In , 4. ACM.

Wills, Craig E, and Mihajlo Zeljkovic. 2011. "A Personalized Approach to Web Privacy: Awareness, Attitudes and Actions." *Information Management & Computer Security* 19 (1): 53–73.

REFERENCES

Akrich, M. 2000. The De-Scription of Technical Objects, In Bijker, W.E. and J. Law, eds., *Shaping Technology/Building Society: Studies in Socio-Technical Change*. Cambridge, MA: MIT Press.

Angwin, J. 2010. The Web's New Gold Mine: Your Secrets. *Wall Street Journal,* July 10. http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404

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

Ayenson, M., Wambach, D.J., Soltani, A., Good, N., and C.J. Hoofnagle. 2012. Behavioral Advertising: The Offer You Cannot Refuse. *Harvard Law and Policy Review* 273.

Beales, H.J. 2013. Protecting Consumers From Privacy Problems: Privacy Issues as 'Unfair or Deceptive Acts or Practices'. *LEC PPC: The Law & Economics of Privacy and Data Security,* June 19.

Beales, H. J., and T.J. Muris. 2008. Choice or Consequences: Protecting Privacy in Commercial Information. *The University of Chicago Law Review* 75(1): 109-135.

Bedi, M. 2013. Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply. *Boston College Law Review* 1.

Benn, S.I. 1984. Privacy, Freedom, and Respect for Persons. In *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, UK: Cambridge University Press.

Bennett, C.J. 2011. In defense of privacy: the concept and the regime. *Surveillance & Society* 8(4): 485-496.

Bentham, Jeremy. 1791. *Panopticon or the Inspection House*. Vol. 2.

———. "Panopticon (1787)." *Jeremy Bentham: The Panopticon Writings*.

Bijker, W.E. 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): 662-679.

Brunton, F. and H. Nissenbaum. 2011. Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation. *First Monday* 16(5).

Buitelaar, J.C. 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). *87 Notre Dame Law Review* 1027.

Calo, R. 2013. Consumer Subject Review Boards: A Thought Experiment. *66 Stanford Law Review* 97.

Cohen, J.E. 2008. Privacy, Visibility, Transparency, and Exposure. *University of Chicago Law Review* 75(1).

Cranor, Lorrie Faith, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au. 2014. "Are They Worth Reading? An In-□depth Analysis of Online Advertising Companies' Privacy Policies." *An In-Depth Analysis of Online Advertising Companies' Privacy Policies (March 31, 2014)*.

Donaldson, T., and T.W. Dunfee. 1994. Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *Academy of Management Review* 19(2): 252-284.

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.

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", *Federal Trade Commission's Fair Information Practice Principles, and the White House's Consumer Data Privacy in a Networked World,* February, 2012.

Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison*. New York, NY: Vintage.

Fried, C. 1970. *An Anatomy of Values*. Cambridge, MA: Harvard University Press.

Hartzog, W. 2012. Chain-Link Confidentiality. *Georgia Law Review* 46: 657.

Hartzog, W. 2012. Reviving Implied Confidentiality. *Indiana Law Journal* 89: 27.

Hartzog, W. and F. Stutzman. 2013. The Case for Online Obscurity *California Law Review* 101: 1-35.

Heeney, C. 2012. Breaching the Contract? Privacy and the UK Census. *The Information Society* 28(5): 316–28.

Hoffman, D. L, Novak, T. P and M.A. Peralta. 1999. Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. *The Information Society* 15(2): 129–39.

Hoofnagle, C.J., and N. Good. 2012. *The Web Privacy Census*, October 2012. http://law.berkelet.edu/privacycensus.htm.

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

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

Kelly, H. 2013. On Data Privacy Day, Twitter and Google focus on Government Requests. *CNN,* January 28. http://www.cnn.com/2013/01/28/tech/social-media/data-privacy-day/

Kerr, O. 2009. The Case for the Third-Party Doctrine. *Michigan Law Review* 107:951.

Kerr, O. 2012. The Mosaic Theory of the Fourth Amendment. *Michigan Law Review* 111(3): 311-354.

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/

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/

Laney, Douglas. 2001. "3D Data Management: Controlling Data Volume, Velocity, and Variety." Gartner. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Langenderfer, J., and D.L. Cook. 2004. Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research* 57(7): 734-747.

Latour, L. 2000. Where are the Missing Masses? The Sociology of a Few Mundane Artifacts, In Bijker, W.E., and J. Law, eds., *Shaping Technology/Building Societies: Studies in Socio-Technical Change*. Cambridge, MA: MIT Press.

Leon, Pedro Giovanni, Lorrie Faith Cranor, Aleecia M McDonald, and Robert McGuire. 2010. "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of p3p Compact Policy Tokens." In , 93–104. ACM.

Leon, Pedro Giovanni, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. "What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?" In , 19–30. ACM.

Leon, Pedro Giovanni, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh. "Why People Are (Un) Willing to Share Information with Online Advertisers."

Leon, Pedro Giovanni, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. "What Matters to Users?: Factors That Affect Users' Willingness to Share Information with Online Advertisers." In , 7. ACM.

Loftus, T. 2011a. Experts Investigate Carrier IQ Fears. *Wall Street Journal,* December 2. http://blogs.wsj.com/digits/2011/12/02/experts-investigate-carrier-iq-fears/

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/

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/

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

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/

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.E. 2012b. Information Technology and Privacy: Conceptual muddles or privacy vacuums? *Ethics and Information Technology* 14(4): 267-284.

Martin, K.E. 2013. Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday* 18:12.

Mayer, J.R., and J.C. Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In *Proceedings of the 2012 IEEE Symposium of Security and Privacy*. Washington, DC: IEEE Computer Society.

Mayes, R., M. Alfino, M. 2006. Limits of Some Formal Approaches to Risk: Directions for Future Research. *Delft University of Technology.*

McDonald, Aleecia M, and Lorrie Faith Cranor. 2008. "Cost of Reading Privacy Policies, the." *ISJLP* 4: 543.

———. 2010. “Beliefs and Behaviors: Internet Users’ Understanding of Behavioral Advertising.” In .
McCole, P., Ramsey, E., and J. Williams. 2010. Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research* 63(9-10): 1018-1024.
Miller, C.C. 2013. Google Says Electronic Snooping by Governments Should Be More Difficult. *The New York Times,* January 28. http://bits.blogs.nytimes.com/2013/01/28/google-says-electronic-snooping-by-governments-should-be-more-difficult/
Moore, E.S., and V.J. Rideout. 2007. The online marketing of food to children: is it just fun and games?. *Journal of Public Policy and Marketing* 26(2): 202-220.
Morgan-Thomas, A., and C. Veloutsou. 2013. Beyond technology acceptance: Brand relationships and online brand experience. *Journal of Business Research* 66(1): 21-27.
Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.
Nissenbaum, H. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140(4): 32-48.
Ohm, P. 2009. The rise and fall of invasive ISP surveillance. *University of Illinois Law Review*, 08-22.
Pariser, E. 2011. What the Internet Knows About You. *CNN,* May 22. http://www.cnn.com/2011/OPINION/05/22/pariser.filter.bubble/
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
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. 197). Why Privacy is Important. *Philosophy and Public Affairs* 4: 323-333.
Regan, P.M. 2011. Response to Bennett: Also in Defense of Privacy. *Surveillance and Society* 8(4): 497-499.
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. *NYU School of Law, Public Law Research Paper.*
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, Katie, and Kirsten E Martin. 2013. “Mobile Privacy Expectations in Context.” In . TPRC.
Sloan, R.H., and R. Warner. 2013. Beyond Notice and Choice: Privacy, Norms, and Consent. *Suffolk University Journal of High Technology Law,* Forthcoming.
Solove, D.J. 2013. Privacy Self-Management and the Consent Dilemma. *126 Harvard Law Review 1880.*
Sprenger, P. 1999. Sun on Privacy: ‘Get Over It’. *Wired,* January 26.

http://archive.wired.com/politics/law/news/1999/01/17538
Stalder, F. 2008. Bourgeois Anarchism and Authoritarian Democracies. *First Monday* 13:7.
Steel, E. 2010. A Web Pioneer Profiles Users by Name. *Wall Street Journal* Digits, October 25. http://online.wsj.com/news/articles/SB1000142 4052702304410504575560243259416072
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/
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/
Strandburg, K.J. 2011. Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change. *Maryland Law Review* 70.
Tene, O., and J. Polonetsky. 2012. Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review* 64:63.
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.
Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." *Available at SSRN 1478214*.
Twitter. 2012. Transparency Report. https://transparency.twitter.com/information-requests/US
Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising." In , 4. ACM.
U.S. Senate. 2013. Committee on Commerce, Science, and Transportation. *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.
Wills, Craig E, and Mihajlo Zeljkovic. 2011. "A Personalized Approach to Web Privacy: Awareness, Attitudes and Actions." *Information Management & Computer Security* 19 (1): 53–73.
Wright, D. 2013. Making Privacy Impact Assessment More Effective. *The Information Society* 29(5): 307–15.