Captive But Mobile:
Privacy Concerns and Remedies for the Mobile Environment

Mihaela Popescu

California State University, San Bernardino, USA

popescum@csusb.edu

Lemi Baruh

Lemi Baruh, Koç University, Turkey

lbaruh@ku.edu.tr

Abstract

We use the legal framework of captive audience to examine the FTC's 2012 privacy guidelines as applied to mobile marketing. We define captive audiences as audiences without functional opt-out mechanisms to avoid situations of coercive communication. By analyzing the current mobile marketing ecosystem, we show that the FTC's privacy guidelines inspired by the Canadian "privacy by design" paradigm fall short of protecting consumers against invasive mobile marketing in at least three respects: (a) the guidelines ignore how, in the context of data monopolies, the combination of location and personal history data threatens autonomy of choice; (b) the guidelines focus exclusively on user control over data sharing, while ignoring control over communicative interaction; (c) the reliance on market mechanisms to produce improved privacy policies may actually increase opt-out costs for consumers. We conclude by discussing two concrete proposals for improvement: a "home mode" for mobile privacy and target-specific privacy contract negotiation.

Keywords: privacy; Federal Trade Commission; mobile; marketing; captive audience; opt-out

On March 26 2012, the Federal Trade Commission (FTC) issued a long-anticipated new privacy framework to meet the privacy challenges posed by the unprecedented demand for, scope of, and means of consumer data collection in the digital environment (Federal Trade Commission 2012b). The guidelines outline best practices for “companies that collect and use consumer data” (iii) and suggest legislative and consumer education initiatives to further address consumers’ privacy needs. The FTC report goes a long way to clarify the privacy standards applicable to the current online and mobile ecosystems characterized by ubiquitous and largely invisible data collection and tracking capabilities. Yet, in this article we will argue that a comprehensive approach to privacy in mobile communication requires the critical examination of privacy principles that go beyond control over tracking and data collection.

In the following, we offer a critique of the FTC framework inspired by the captive audience legal paradigm. To be sure, the image of consumer “captivity” emerging from our analysis is not confined to a specific, clearly delineated communicator-audience interaction, as a court would demand. Instead, we use the captive audience doctrine as a lens through which to identify emerging features of the contemporary digital and increasingly mobile communication environment that pose privacy concerns, and analyze the FTC’s privacy guidelines against this background of digital and mobile marketing practices. We submit that the captive audience doctrine invoked in this article provides insight into an alternative approach to privacy informed not by the “context of interaction” standard that the FTC adopted, but by the “context of communicative interaction” standard that the captive audience caseload suggests. This standard would enable individuals to control not only the flow of information about themselves, but also the flow of communication targeting them. We will argue that the FTC “context of interaction” standard focuses exclusively on privacy as data appropriation and private data disclosure, while

not sufficiently addressing the larger issues of consumers' autonomy in communicative interactions and their choice of solitude over public communication. Additionally, we will argue that a possible unintended effect of the new privacy framework will be the creation of incentives for more horizontal integration in the mobile market for the purposes of creating privacy lock-ins.

Following a review of the FTC's new privacy guidelines, we examine the captive audience legal doctrine for its insights it provides regarding the core privacy values to be protected against unbridled marketing communication. Next, we show how the FTC's new approach to privacy inspired by the notion of "privacy by design" falls short of protecting consumers against a ubiquitous "mobile captivity." We conclude by discussing why the insights provided by the captive audience doctrine should be incorporated into future privacy regulations, and what those insights suggest in regard to designing meaningful "privacy interfaces" able to restore users' control over both their information and their communication flow.

The 2012 FTC Privacy Guidelines

The new FTC privacy framework (2012b) is meant to apply to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share data with third parties" (22). Even though it is neither directly enforceable, nor does it represent a template for enforcing current FTC regulations, the Report is notable for its aims to inform legislative efforts in Congress and for its recognition of "the complexity of the current personal data ecosystem" (7). Noting that "consumers face a landscape of virtually ubiquitous collection of data" (18), the Commission stressed the current privacy vulnerabilities of consumers in both online and offline commercial contexts. The

Commission did not offer a formal definition of sensitive data, but did give examples of what might come under this label. Significantly, in addition to expected candidates such as the Social Security Number, financial and health-related data, and data collected from children, the FTC included “precise geolocation data” (59) in the category of “high risk” sensitive data.

In the Report (2012b), the Commission acknowledged that “the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions” (8) insofar as it may include the unauthorized disclosure of sensitive and non-sensitive consumer data to unknown third parties. The new FTC privacy approach may be qualified as innovative both in regards to its scope and in regards to the three baseline principles it proposes: 1) privacy by design on the companies’ side, 2) simplified consumer choice for data transactions, and 3) more transparency, including consumer education.

The first principle that the FTC adopted is the “Privacy by Design” framework proposed in 2008 by Ann Cavoukian, the Head of the Ontario Information and Privacy Commission in Canada. The essence of this principle is to think of privacy proactively at the technological design stage and throughout the life-cycle of the product (The Toronto Star, March 3, 2012). In the FTC version (2012b), companies are called upon to “promote consumer privacy throughout their organization and at every state of the development of their products and services” (22). This approach would presumably influence both a revised organizational logic (for example, creating new positions for ensuring compliance with the adopted best practices) and induce new, risk-averse approaches in handling consumer data, such as limiting data collection to data “consistent with the context of a particular transaction” (27) or by implementing limits on data retention.

A second principle articulated by the new FTC framework is simplified consumer choice, translated into a new “context of interaction” standard that spells out under what conditions, at

what moment in the transaction, and in which form companies should provide privacy choices for their customers. The context of interaction standard depends on customers' reasonable expectations of privacy when entering a transaction with a party, and revolves around the distinction between first-party interaction, that is, a business-to-consumer transaction, and a third-party interaction, in which the original company buys or sells data about the consumer, or otherwise uses it in a context not consistent with the terms of the transaction.

According to the FTC (2012b), under this context of interaction standard, third-parties are any company affiliates whose relationship with the company is not clear to consumers (42). Thus, when a company engages in a data use practice, such as first-party marketing or cross-channel marketing, that is consistent with the context of transaction or customer's previous business relationship with the company, such practice would not warrant the provision of additional privacy choices. In contrast, tracking consumer activity in contexts not consistent with the provision of the service agreed on, or across third-parties' websites, such as the practice of "retargeting" whereby companies deliver personalized ads on third-party websites based on the purchase history of their consumers, would require meaningful consumer choice. In particular, the Commission supported the Do Not Track industry efforts as a means to provide meaningful choice to consumers, and underlined choice by specifying that a Do Not Track system should allow consumers to stop the collection of behavioral data about themselves. The FTC specified that consumer choice needs to be provided "at a time and in a context in which the consumer is making a decision about his or her data" (48), although the companies would still have considerable latitude about the format in which to present the choice, or exactly when to communicate the choice. The Commission also discouraged the "take-it-or-leave-it" types of privacy contracts in a market with few consumer options. The FTC expressed particular concern

about large platform providers such as ISPs, operating systems or browsers, but interestingly, not Google or Facebook, considered “not so widespread that they could track a consumer’s every movement across the Internet” (56).

The third and final principle underpinning the FTC’s new privacy framework (2012b) would require companies to increase the transparency of their data practices through better privacy notices, increased consumer access to personal data collected by a company, and provide better consumer education. The Commission recommended clearer, shorter and more standardized privacy statements. As applied to the mobile ecosystems, the Commission noted the urgent need for “standard notices, icons, and other means that the range of businesses can use to communicate with consumers in a consistent and clear way” (64). Standardization would enable consumers to compare and contrast privacy practices across digital providers, and would encourage companies in the digital environment to compete on privacy. As such, this principle transforms privacy into a product, thus creating a market for privacy.

Additionally, the Commission recommended that companies inform their customers about the categories of personal data used by a company and the sources of such data, and grant access to consumers to modify or delete data used for marketing. The FTC (2012b) explicitly stated support for legislation granting “access rights to consumers to information held by data brokers” and recommended that data brokers create a centralized website to identify themselves to consumers, disclose their data collection practices and their business partners, provide data access to consumers, and provide choices to consumer regarding their data (69-70). Finally, the Commission called on companies to step up their efforts to educate consumers about commercial data privacy practices, and cited OnGuardOnline.gov website, created in partnership with 15

federal agencies, as a good repository of a wealth of material raising consumer awareness of online privacy issues.

The Captive Audience Doctrine

In what follows, we employ the captive audience doctrine developed at common law both as a source of insight for our criticism of the FTC framework, and as an organizing tool for discussing the characteristics of the mobile marketing environment. We use the captive audience doctrine to pose the questions the FTC recommendations left unasked, and posit that both scholars and policy makers should consider those questions more seriously when examining the privacy implications of the mobile computing environment.

This reference to the captive audience doctrine is quite appropriate because current privacy initiatives mirror past regulation inspired by captive audience claims. For example, the Do Not Track industry initiative, which provides technology that enables online and mobile users to opt out of third-party web tracking, mirrors the Do Not Call Registry. The Do Not Call Registry is a joint FTC and Federal Communication Commission (FCC) effort that allows customers to put their numbers on a national registry if they do not wish to receive telemarketing calls, and provides penalties for telemarketers who ignore that choice. In establishing the legitimacy of the Do Not Call initiative, the Court of Appeals for the Tenth Circuit recognized the unwilling listener's interest to avoid unwanted communication, the interest of the government in protecting the privacy of individuals in their homes, and the burden that will be placed on consumers to "compete in a technological arms race with the telemarketing industry" should the government fail to intervene.¹

The concept of "captive audience" emerged in common law as a legal mechanism to protect audiences against intrusive speech, in particular intrusive commercial speech.² The first

use of the term “captive audience” by Justice Douglas in a famous 1952 dissent described the situation of bus commuters forced to listen to commercial messages over the bus transit radio.³ In Justice Douglas’s view, the First Amendment did not protect communication that intruded on the solitude of bus passengers, who had no way to avoid message exposure other than giving up on the bus commute. Since then, the captive audience paradigm has been invoked with various degrees of success in a wide range of situations, such as commercial⁴ or religious⁵ solicitation, direct marketing⁶, public address systems⁷, billboards and other public thrusting⁸, protests⁹, residential picketing¹⁰, or indecent broadcasts¹¹.

From Warren and Brandeis’ “right to be let alone” to the Supreme Court ruling in *Snyder v. Phelps* (2010), the concept of “captive audience” came to refer to a situation in which communicators appear to “force” their messages on audiences unwilling to listen, absent meaningful choices for avoiding communication. This right offers a cause of action enabling relatively powerless audiences to prevent unwanted intrusions. Although the First Amendment places paramount importance on the right of speakers to communicate their ideas, a situation involving captive audiences allows the government to intervene on their behalf and protect their privacy rights through regulation that limits the reach of certain forms of communication.

The basis of a captive audience claim is the identification of contexts in which the communicative act is such that its intended target cannot avoid it. “Captive audience” refers precisely to a situation in which, owing to a lack of choice, the communicators appear to “force” their messages on audiences incapable to avoid them. The idea of a power differential between communicators and audiences is best conveyed through some of the metaphors judges employed in their rulings: messages are “thrust upon” observers¹² or represent “a verbal [or visual] assault”¹³; speakers “force [their] message”¹⁴ which, in turn, may “inflame the sensibilities” of

the receivers¹⁵, whose attention is “bludgeoned” by undesired speech.¹⁶ In these cases, ruling in favor of a captive audience claim depends on showing that “substantial privacy interests [are] being invaded in an essentially intolerable manner,”¹⁷ and supporting a captive audience claim means favoring the privacy interests of the listeners over the First Amendment rights of the speakers. At stake in captive audience cases is not the right of private action against unwanted communication, but the legitimacy of the state to limit certain forms of communication in order to protect audiences’ privacy.

Despite its application in a wide range of cases, the captive audience doctrine is fraught with tensions insofar as its interpretations reflect conflicting views of precisely what type of communication the captive audience doctrine protects against, and in what situations. At least two reasons increase the difficulty of harmonizing cases. One has to do with the nature of the communication act. The rulings in captive audience cases pertain to messages that are unwanted (as in cases involving unwanted mails or telemarketing calls), overwhelming to senses (as in cases of public addresses over loudspeakers), offensive because of their content (as in cases involving unexpected exposure to erotica or indecent messages) or emotionally harmful (as in cases involving residential picketing, anti-abortion or other protests). Although in all these cases an unwanted message is “thrust upon” an unwilling audience whose otherwise legitimate activities are thus interrupted, it is difficult to articulate the common underlying harm and the normative principle to be adopted herein (Haiman 1972). Moreover, because the type of speech differs across cases, the nature of the First Amendment analysis differs as well.

A second reason why harmonizing the caseload is troublesome pertains to the variety of locations where unwanted communication acts occurs, such as private homes, sidewalks, schools, sports stadiums, buses, parks or other public spaces. Although place in itself may be

relevant only as “a shorthand for the possibility of communicative interaction” (Jacobs 1998, 518), the result of balancing speaker and listener rights differs across locations. Since First Amendment protections are at their highest in public forums, more often than not, the outcome of a forum-based analysis is to only rule in favor of the captive audience when speech occurs on an individual’s private property such as one’s home.¹⁸

Our reading of the captive audience caseload suggests that neither place, nor speech type, nor indeed an audience’s attitude toward a message are good indicators of when a captive audience claim is warranted. Rather, at stake in captive audience cases is who has more control over the context of communication. Whether or not a message is considered offensive to audiences’ privacy depends entirely on the context of message reception as defined by the ability of audiences to exercise autonomous choice of whether or not to receive the message, their privacy expectations given the communicative context, and the existence of functional opt-out mechanisms enabling audiences to exit the communicative context without costs to themselves. Although in practice these factors may overlap (for example, sometimes a structural lack of functional opt-out mechanisms is in fact the reason why audiences cannot exercise choice), neither factor is in itself sufficient to warrant a captive audience claim.

The notion of autonomous choice in the context of the captive audience doctrine requires some discussion. Communicators may have the power to force a choice and thus override audiences’ autonomy in several ways. For example, autonomy of choice may be non-existent when audiences are vulnerable to start with, as children are often considered to be. Children’s refusal to hear a message often comes with explicit penalties. Moreover, children do not have the ability to distinguish between mere suggestions (persuasive messages) and actual orders (coercive messages). Communicators whose social power over audiences is high, for example employers

communicating with employees, make adult audiences equally vulnerable to communicative coercion simply because they do not have the power to refuse listening to, let alone to refuse to follow, the communicators' suggestions (Balkin 1999). The Court has implicitly recognized the existence of communicative situations that render audiences "child-like" in regard to their ability to exercise choice by refusing communicative engagement.¹⁹ We add that the same considerations of choice autonomy apply to situations when audiences are turned vulnerable by life events or special circumstances about the communication act, for example in situations of recovering after accidents, undergoing an abortion, or mourning at funerals (Balkin 1999; Brownstein and Amar 2010), because audiences are less likely to weigh arguments dispassionately in those contexts. A relevant example, by no means unique, of situations when audiences become vulnerable due to life events corresponds to what anthropologists call "liminal states," namely, periods of transition in which individuals move from one life stage to another.

The liminal state has an important function in the formation of individual identity. In anthropology, van Gennep (1909) used the term to refer to intermediary states in the coming-of-age rites of passage of tribal cultures whereby individuals needed to isolate themselves from the community in order to transition from one status to another, for example from unmarried girl to married woman. Turner (1974; 1967) expanded van Gennep's definition to modern societies and described liminality as a transitional state of isolation within which individuals "betwixt and between" social structures give up their older status and retreat from society in the process of acquiring a new status by means of which their reintegration in society is achieved. As applied to individual identity, Jung and his followers (1953, 227-241; Hall 1991) saw a parallel between the concept of social liminality and integration of opposing trends in one's personality into a unitary whole. The importance of what we called liminal states for altering ingrained individual

behaviors is well known to markets. For example, in a much publicized scandal, Target, which understood that the shopping habits of female customers were particularly flexible during, was able to predict so well the likelihood of a consumer being pregnant, that it correctly targeted a pregnant teenager whose father only found out about his daughter's condition from Target baby cloths coupons (Duhigg, 2012). Importantly, then, protecting individuals in liminal states may be interpreted as protecting their autonomy, including their autonomy when making life-altering choices.

The Supreme Court has indirectly recognized the existence of such crucial moments in the lives of individuals and the state's interest in protecting individuals' autonomy of choice at such moments: "[a]t the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life."²⁰ Thus, in cases involving targeted protests, the Supreme Court recognized the so-called "privacy of choice," namely the need to protect an individual's capacity for rational decision when the circumstances coerce the audience to accept views "for reasons entirely unrelated to the audience's rational, conscientious, or autonomous capacity" (Lederman 1995, 1299).

Thus, we agree with Balkin (1999) that the focus on place in captive audience cases is simply a convenient device to refer to a nexus of power and asymmetric dependence, and that the captive audience doctrine should regulate on "particular situations where people are particularly subject to unjust and intolerable harassment and coercion" (2312). In such situations, individual First Amendment rights to mental autonomy, that is, the right to hear or see what one wishes, reinforce the privacy right to one's voluntary seclusion and consequently one's right to personal autonomy. In this sense, the notion of captivity recognizes that audiences are unable to exit a communicative situation that threaten their mental autonomy without harm to themselves in the

form of economic loss, significant inconvenience, or emotional distress; the normative principle behind captive audience regulation is that they should not have to quit at all (Corbin 2009, 943-944).

For the purpose of our privacy analysis, we define captive audiences as audiences without functional opt-out mechanisms to avoid situations of coercive communication. By coercive communication we understand communication addressed to audiences that are turned vulnerable by the conditions of message reception. As explained above, the conditions of reception that might render audiences vulnerable include considerations of whether audiences are capable of autonomous choice given the audiences' expectations of privacy and their comparative power to enforce those expectations. By functional opt-out mechanisms we mean mechanisms which, under agreed-upon expectations of privacy, audiences are capable of using without significant costs to themselves. Thus, our definition has three distinct elements: (a) the ability of audiences to exercise autonomous choice in regard to a message; (b) the nature of audiences' privacy expectations; (c) the existence of functional opt-out mechanisms.

The following discusses each element of the definition in the context of mobile marketing. We examine how (a) contextual mobile marketing problematizes the meaning of autonomous choice, how (b) mobile communication blurs the context of social practice on which privacy rights were previously articulated, thus rendering privacy expectations ambiguous, and how (c) new consumer locks-in induced by mobile business models increase costs on consumer opt-out. We critique the FTC recommendations for reducing individual autonomy to data autonomy, failing to articulate privacy expectations, and transforming privacy into a market product, thus creating new forms of consumer lock-in.

From Unwanted Messages to Coercive Communication

The first element of our definition of captive audience pertains to individuals' ability to exercise autonomous choice while making decisions that may impact their lives. Admittedly, the new FTC recommendations go a long way in remedying the imbalance of power between individual users at one pole, and the industries in the data ecosystem, such as publishers, data brokers, ad networks, or media metrics companies, at the other. However, it is notable that in the FTC report individual autonomy is narrowly equated with data autonomy, whereas the right to be let alone protects individual autonomy in a broader sense, including autonomy of choice free from constraining influences (Baruh and Popescu 2010).

Considered from this perspective, the new privacy recommendations play right into the rhetoric of better customization through more extensive data collection which content providers have promoted since the early days of the Internet (Andrejevic 2007; Turow 2011). As the argument goes, consumers give up a certain amount of privacy in exchange for better tailoring of commercial content, which spares consumers the burden of unwanted advertising that interrupts their media experience. In particular, mobile marketers have brought the rhetoric of consumer choice to new heights by touting the ability of the mobile web to deliver messages in perfect resonance with consumers' every mood. Content delivered at the right time, in the right place, when the consumer is in the right mood brings a literal meaning to the Holy Grail of marketing, namely, marketing to "a segment of one" (Albert 2011).

Thus, if we were to persist in understanding captive audience situations as entirely dependent on the content of communicative address or the method of its delivery, marketers could easily argue that targeted content is the very antithesis of unwanted content. In this context, the main regulatory problem, as illustrated by the FTC report, would only be to protect the process wherein users make their choices known to content providers. However, as illustrated

below, the emerging mobile ecology potentially enables customization of content and method of delivery to such an extent, that it is now plausible to imagine advertising delivered to mobile users at the precise moment they are most likely to be persuaded, for example during particular times in their lives that meet the definition of liminality discussed above. By identifying contexts of reception when audiences become vulnerable to persuasion, marketers erode their customers' autonomous choice that the captive audience doctrine protects. The following analysis shows how elements characteristic to mobile marketing, such as the ability to collect and mine locational data, lead to message tailoring that problematizes customers' ability to exercise autonomous choice.

In the mobile environment, the new height of message tailoring is possible thanks to contextual marketing enabled by location-aware mobile devices and data linkages across all levels of consumers' activities. Contextual marketing is different from locational marketing. Locational or proximity marketing, as implemented by platforms such as Foursquare, Yelp, Gowalla or Loopt, is a type of marketing that allows users, who share their physical locations via their mobile devices, to receive commercial offers tailored to the particular place they are in. In contrast, contextual marketing targets more than geographic location. Although the idea behind contextual marketing is not new, what is new is the ability of mobile marketers to actually implement context-targeting by accumulating dynamic knowledge about a user's habits and the "web of meanings" that surround those habits (Silva and Frith 2012, 111-135). The point is not simply to collect data about consumer location, but to relate data thus collected to the meaning it holds for users, and to the context the users are in. Gary S. Laben, CEO of the marketing solutions provider KBM Group, expressed this idea as follows: "The old buying model - i.e., RFM: Recency, Frequency, Monetary [asked about customers] 'When did I buy last? What did I

buy? And how much did I buy?'...Now, it's about, 'Where am I at the moment? What is it that I'm purchasing right now? And with whom am I conversing at that moment?'" (quoted in McGee 2011). Marketing to context goes beyond proximity marketing by involving a relational approach that combines "a person's location, inferred intent and personal affinities to aggregate and deliver relevant information about the real world surrounding them at any given moment" (Klaassen and Patel 2009).

In short, when related to a user's home, place of work, and personal habits, geographical coordinates transform the location into a "place." For marketers, it is not enough to know the geographical coordinates of the mobile user, but to make inferences about how those coordinates relate to a user's home or place of work, and to a user's personal habits (Albert 2011; Klaassen and Patel 2009). Thus, the big promise of the location-sharing platforms for marketers is the ability to better target users by collecting relational information and combining location filters with other social filters (tweets, Flickr photos, etc.) that give off important cues about the significance of location for the users.

Additionally, locations may become significant in light of individuals' history. Tailoring messages based on a combination of meaningful moments and the "right" locations produces hard to resist advertising messages, because life event triggers, such as the liminal moments we discussed above, are some of the most reliable predictors of consumer buying behavior (DeMartine 2011). Indeed, as brands such as Modern Bride or American Baby well know, some of the most successful marketing campaigns tap into the marketers' ability to identify consumers during "liminal," transitional times such as right before getting married or while expecting a baby, when consumers are at their most vulnerable. Thus, the combination of social filters that Google, among others, controls, namely "the social graph (contacts, friends), interest data (likes,

tweets, recommendations), search data (queries, history), purchase data (what you buy, credit card numbers), location data (where you are, have been, and are going), and content data (behavior when engaged with content)” (Claburn 2011), produce a new category of social data with unprecedented marketing potential.

These situations illustrate how the combination of location knowledge and knowledge about an individual’s history produce heightened levels of corporate surveillance (Silva and Frith 2012, 111-135) that directly harm the autonomy of individuals, one of the values that privacy arguably protects.²¹ Particularly during times when life events render individuals less likely to critically evaluate the persuasive intent of incoming messages, such an ability to predict individuals’ preferences may result in what Zarsky (2004) describes as autonomy traps, namely the process whereby institutions increasingly design messages according to what individuals are more likely to accept rather than what they actually need to make an informed decisions. In this context, FTC’s focus on consumer control over marketing categories should be supplemented with an acknowledgement of the coercive communicative potential of social data monopolies. FTC’s special concern for ISP’s and mobile providers, but not for social platform owners such as Google, Apple or Microsoft, seems curiously misplaced. Quite the contrary, social data, rather than service usage data, are better positioned to produce coercive communication of the type a comprehensive privacy framework should protect against.

Mobility and Privacy Expectations

The second element of the captive audience doctrine, implicitly recognized by our definition, pertains to the assertion that intrusive communication, be it telemarketing phone calls, residential protests, or fleeting exposure to erotica in a drive-in theater, violates the term of a (usually unwritten) “privacy contract” wherein audiences are entitled to their undisturbed

solitude by virtue of commonly accepted privacy expectations. As discussed before, because the large bulk of the captive audience caseload relied on spatial conceptions of captivity, the social expectations of privacy recognized in judicial discourse have been to a large extent place-dependent (Zick 2007, 28). Thus, intrusion upon solitude, identified by Prosser (1960) as a facet of privacy, gained material embeddedness by association to particular locations and became closely related to the regulating function of physical space, and particularly the home, as a marker of (in)accessibility, ownership and control, and (un)acceptable forms of social exchange (Marcus 1998, 300; Marx 2001).²²

However, as many scholars observed, each new form of mediation or communication technology or practice, such as marketing materials in mailboxes, unsolicited telemarketing calls or fax transmissions, or unsolicited junk email, challenged the formerly (and relatively) clear-cut private/public border both socially and legally (Marx 2001; Shapiro 2006). As Nissenbaum (2010) argues, in digital contexts privacy expectations no longer map easily onto the private/public dichotomy because the dichotomy neglects both the legitimacy of privacy expectations in certain public situations, and the variety of public and private actors involved in data collection and use. Likewise, the penetration of mobile and interactive technologies into the regular lives of individuals further blurs this already ambiguous distinction between private and public (Lievrouw and Livingstone 2002), thus rendering privacy expectations ambiguous. Additionally, mobile technologies problematize the privacy expectations of device-holders in public places (Silva and Frith 2012). Therefore, the redefinition of privacy expectations invited by mobile technologies creates a need to reconsider the contexts of communication in which mobile device users may rightfully claim a need for privacy protection. This argument, though not new, has profound implications on the legal recognition of communicative situations in need

of privacy protection, on the type of signals individuals may use to indicate the beginning and end of such situations, and on the types of social boundaries those signals constitute. In this section, we examine some tensions in the construction of privacy expectations about mobile communication, and argue that a holistic privacy framework should take into account not only individual control over the exchange of information in a transaction, as the FTC framework proposes, but also individual control over the social boundaries regulating who is allowed to address the individual, for what purposes, at what times, and using which tools and advantages.

As indicated above, for the “always on” mobile users, domains such as home, work, school, or shopping mall, traditionally considered to be separate from each other and analyzed as such in legal discourse, are increasingly becoming indistinguishable. Moreover, with the wide adoption of smart devices allowing access to information clouds irrespective of one’s location, the distinction between virtual and material places, online and offline, is starting to disappear as well (Zick 2007, 13). It is within this context that Sheller and Urry (2003) criticize reliance on concepts such as space or sphere, which they characterize as being too static, to distinguish between private and public moments.

It is not that places do not exist anymore but rather, as Castells (2007, 172) argues, places “exist as points of convergence in communication networks.” Under conditions of ubiquitous connectivity, it is communication availability, rather than physical spatiality, that determines the meaning of places. For that reason, Castells proposes the notion of “flow”—metaphor suggestive of an intersection of spatial mobility and temporal processes—as the unit of interaction between mobile users and their environment. The concept of “flow” is particularly apt to acknowledge that the meaning a certain place holds for an individual may change as a function of the individual’s situation in a particular moment in time, and thus individual privacy needs do not

map directly and easily onto a spatial or temporal grid. In other words, as Cohen (2008) argues, the spatial dimension of privacy is not merely about the accessibility of physical space, but rather about individuals' ability to selectively control the "conditions of exposure" (194).

Indeed, as cross-cultural research on privacy amply demonstrates it seems to be a universal constant that our privacy expectations are grounded in social relations and unwritten social conventions. For example, Adams, Murata, and Orito (2009) argue that much of the recent laws regarding informational privacy in Japan have their basis in traditions regarding interpersonal relations. One such tradition is the *as-if* tradition. This tradition is closely linked to the material used to construct walls (paper or light wood) in Japanese houses. Since these walls did not allow much insulation between rooms, the *as-if* tradition meant that when an information "was overheard but not explicitly given, is treated as if one did not have it" (4). To a great extent, for the *as-if* tradition, which reflects the general tendency in Japanese culture to distinguish between "inner" and "outer" circles, it is not solely the physical space but also the context of communication that determines the distinction between inner and outer circle.

Western cultures include privacy conventions very similar to the *as-if* tradition. For example, Goffman's (1963) concept of *civil inattention* underlines how strangers cohabiting a space recognize each other's presence as a courtesy, but then try to remain unobtrusive and signal the existence of a boundary. Similarly, Nagel (1998, 8) argues that conventions regarding the *nonacknowledgement* of certain wishes, thoughts, issues or feelings are key to maintenance of social interactions because accepting people as they are requires that we recognize "there is more to them than could possibly be integrated into a common social space." In our daily lives we regularly face situations that require civil inattention or nonacknowledgement. One of their main functions is to protect the privacy and public faces of individuals by differentiating between

types of behaviors that call for extra attention and types of behavior that we should avoid noticing (Nagel 1998). Again, it can be observed that the norms associated with civil inattention or nonacknowledgement have as much to do with the communicative context (e.g., who is the intended and unintended recipient? what is the form of communicative behavior?) as the physical place within which the communication takes place. For example, social conventions often indicate that emotions, and particularly negative emotions are a private matter with backstage bias and should be accessible only to the right people (i.e., loud quarrels between spouses would be out of “place” both in a public bus and at a private dinner party with friends) (Ekman and Friesen 1969).

The discussion above serves to show that the reliance on physical place in much of the legal discourse about privacy is often but a proxy, albeit imperfect, for determining whether audiences have at their disposal clear and decodable signaling mechanisms indicating that a communicative act is not welcome at particular times.²³ It is in this context that Standburg (2011) proposes technosocial continuity as a principle that should be used to determine the circumstances when the privacy of the “physical home” should extend to online communication. Although Standburg’s proposal addresses the extension only in narrow conditions, the principle of technosocial continuity underlines how a comprehensive privacy framework would need to restore individual control over the context of communicative interaction by enabling the individual to “broadcast” social signals indicating the individual’s desire for privacy. If, for privacy purposes, “home” is in fact a legal proxy for maximum privacy expectations, we need to rethink what constitutes “home” in the context of mobile communication.

The problem is complicated by the fact that, for device-mediated communication, the meaning of consumer signaling mechanisms is significantly and quite deliberately left

ambiguous. For example, an opt-out act such as unsubscribing from communicative contact with a commercial party via the mechanism provided by that party itself does not automatically imply the end of the commercial transaction, as the party may legally continue its data collection activities. Conversely, a consumer's opt-out from data collection by a commercial entity does not imply that the party will cease communication with the consumer or will stop targeting the consumer with marketing messages. Consequently, the opt-out approach at the core of the Do Not Track self-regulatory initiative is insufficient to grant the full user control over the context of communicative interaction, as the older Do Not Call legislation did. Similarly, the "context of interaction" standard proposed by the FTC may protect users against third-party data collection, but does not restore users' control over the communicative interaction with the original party. In addition to the centralized data broker website that puts the onus on the consumer to identify and modify the categories that marketers use to define her, the FTC needs to define and enforce "privacy regimes" recognized by marketers and data brokers by means of which consumers may indicate unambiguously the level of privacy they desire at particular times.

Lock-ins and Exit Costs

In this section, we discuss to what extent audiences have functional opt-outs from online and mobile marketing. Since 1998, the FTC has relied mostly on a combination of a market-based approach and self-regulation enforcement to protect online consumer privacy (Park 2011). Similarly, the 2012 FTC report explicitly frames privacy as a market product to be competed over. However, it is not clear what kind of incentives would drive companies to outperform their competitors in respect to their privacy practices. In order for the market model to successfully produce improved privacy practices, users need the ability to make a choice among competing businesses (Swire 1997). The self-management privacy model which assumes that a rational

consumer will drop a company with poor privacy practices and switch to a better competitor relies on market preconditions that presuppose that privacy violators are readily identifiable; that consumers routinely read privacy policies, are able to understand and compare competing policies; and that consumers are able to quit transactions with a company whose privacy practices are not up to par.

So far, these preconditions have not been fulfilled in practice. Recent privacy scandals that involved deceptive online data collection, for example Google's practice of placing tracking cookies on the Safari browser despite claims to the contrary, demonstrate that a lay user would need highly specialized technical knowledge to identify privacy violators (Felten 2012). Studies show that less than a third of online users read, however partially, a website's privacy policy (McDonald et al. 2009, 37), with only about 2% likely to read it thoroughly (Turow et al. 2007, 740). Moreover, studies also demonstrate that privacy policies are confusing to users (McDonald et al. 2009; Turow et al. 2007; Kelley et al. 2009, 2010) and that users have real difficulties comparing competing privacy policies, not least because of their lack of standardization (Turow et al. 2007; Kelley et al. 2009, 2010).

To partly remedy this situation, the Commission recommended that companies “standardize the format and the terminology used in privacy statements so that consumers can compare the data practices of different companies and exercise choices based on privacy concerns, thereby encouraging companies to compete on privacy.” (61) This initiative reproduces the neoliberal logic that favors self-regulation over state intervention and promotes market competition over social need by concentrating on the supplier side, instead of increasing user control and regulating information asymmetries (Schiller 2007, 61)—for example, by

introducing standardized “privacy nutrition label” (Bonneau and Preibusch 2010, 162; Kelley et al. 2009) with state—rather than company-defined—categories.

Even if a standardized privacy policy were to become the industry standard, in the context of the captive audience doctrine used in this article, the assumption that users will easily be able to switch digital platforms if dissatisfied with a company’s privacy policy and subsequent marketing practices is highly suspect. The point is not that users lack available means of refusing engagement with marketing communication, but that, given the current economic setup of the mobile environment, the material and immaterial costs incurred by a user for disengagement render these opt-out mechanisms costs-prohibitive for the users. We explore forms of digital lock-ins as the last prong of our captive audience definition. Although our discussion is applicable to digital environments in general and not necessarily confined to mobile environments, we show how the latter create additional lock-ins that reduce the ability of audiences to opt out of both data collection and marketing communication.

According to Shapiro and Varian (1999, 103-134), lock-ins, namely, the costs incurred by customers when switching from a product to a competing product, are ubiquitous and normative in the information society. Switching costs may include, but are not limited to, financial costs; they also pertain to social, psychological, situational, and time-related costs that a customer needs to pay in order to migrate from one brand or service to another (Dick and Basu 1994). Any buying contract with a provider specifying the damages to be paid by the buyer when switching providers before the contract expired is a form of lock-in. Loyalty programs such as flying miles or annual rebates are also lock-ins mechanisms that aim to create disincentives for customers to abandon a commercial relationship. Similarly, the time invested in learning to operate a piece of equipment discourages users from switching to different equipment and ensures a loyal customer

base for the equipment suppliers. However, unlike physical equipment whose obsolescence might encourage users to contemplate its replacement with a better alternative, the economic and legal arrangements of the digital environment produce forms of durable lock-ins that increase, rather than dissolve, over time. The example of the Digital Rights Management (DRM) systems will serve to make the point.

Generally, DRM systems have two related functions. The first is to assign a unique identifier—typically in the form of fingerprints or watermarks—to a certain content so that the file can be traced back to the user to prevent widespread sharing (Benoliel 2004; Godwin 2004). The second function of DRM systems is to mechanically dictate copyright claims about how users can use a specific content file (Bell 1998; Burk and Cohen 2001). Typically, the second function of DRM systems is intended to strictly govern a number of user-related behaviors such as transferring (between different platforms) or copying content as well as transforming content (e.g., editing) for creative purposes (Fetscherin 2006).

The second function of digital rights management systems play a key role in regulating consumption behavior regardless of the domain within which it takes place and its actor (Lessig 2004). At the most immediate level, DRM creates sticky relationships between users of cultural objects and content/technology providers (and intermediaries). First, proprietary in nature, none of the DRM systems have actually become the industry standard in the market place, creating many different systems, most of which are not interoperable with each other. Second, and as a result of the first characteristic, most DRM systems make it cost-prohibitive for customers to switch between systems by locking in content to specific number of devices (e.g., Microsoft Zune Marketplace music with DRM is compatible only with the soon-to-be-discontinued Zune devices).²⁴

It is important to note that this “cultural artifact-supplier-delivery media” lock-in created by DRM systems changes the relationship between content suppliers and users. Namely, a user’s download of a media file does not transfer ownership of the content from the service provider to the consumer, but rather constitutes a retractable granting of usage rights and user limitations enforced both legally, through licensing, and technologically, through DRM mechanisms. Thus, the combination of licensing and DRM mechanisms ensures that users are “tethered” to particular content providers and may, at most, supplement their content libraries with content from different providers, rather than replace those libraries altogether.

The example of the DRM lock-in is among the most visible and contentious, but it is by no means a unique case. By developing everyday practices around digital artifacts and platforms, users implicitly and uncritically accept a myriad other lock-in situations that ensure their loyalty to digital products and service providers. The mobile industry is no exception. Mobile providers use various technological constraints and tie-in arrangements with device-makers and mobile operating system owners to lock-in users as a way of preventing them from switching to competing products. At the simplest level, mobile phones activated on one cellular service provider’s network will not accept a SIM card from competitors and thus will work only on that network (Greenhalgh 2008, 443-444). Major cellular providers, AT&T, Verizon, T-Mobile and Sprint, provide customers with free handsets and customizable data plans that offer free minutes or free messaging capabilities, but also hefty contract termination fees in addition to the loss of accumulated benefits. Indeed, research on the mobile market shows that among switching barriers, subscriber lock is the most significant factor that discourages mobile subscribers to change carriers (Shin and Kim 2008).

Importantly, customization and personalization are but another form of lock-in (Bonneau and Preibusch 2010; Chellappa and Sin 2005). Bonneau and Preibusch (2010) successfully demonstrated the relationship between increased customization and stronger lock-ins for the case of social networks. For example, users spend a significant time creating their profiles on social media sites and learning the interfaces, but their profile data and the networks they build are lost if they migrate to a different social network; applications that offer to retrieve old profile data, such as Google's FriendConnect service, are prevented from doing so through technological and legal means. For that reason, the more effort users invest in developing a social network, the less likely they are to migrate to a different one. At this point, it will probably be clear to any user of a social network site such as Facebook that the sticky relationship created by social media is often less about the availability of comparable applications to create profiles than about the improbable task of migrating one's actual network of friends across platforms.

Similar considerations of customization as lock-in apply to mobile devices. More than computers, mobile devices are increasingly embedded in their users' lives because the mobile apps installed on these devices fulfill a variety of functions. Just like social media platforms, mobile apps are also marketing platforms because they enable both the collection of data of about users, and act as delivery channels for marketing messages. More than social media platforms, mobile apps present opportunities to create personalized brand-to-customer relationships by creating loyalty programs and offering coupon and in-store discounts (Davis 2012). However, because the major manufacturers of mobile devices also have proprietary mobile operating systems, the apps that enable mobile functionalities are also specific to the operating system, so that customizing a mobile device comes with both time and money investment. Thus, switching to a different mobile manufacturer means not only changing the

mobile device, but also abandoning an entire mobile ecosystem. Indeed, corporate strategies of companies increasingly underline how integration of the “social” and “mobile” components of digital ecosystems is key to locking in customers. For example, a study by GFK suggests that more than 50% of owners of Apple’s mobile iOS devices (iPad and iPhone) would not consider switching to other mobile ecosystems because they did not want to deal with migrating applications or (social) content (cited in Kahn, 2011).

We noted at the beginning of this section that the argument that market competition may allegedly produce better privacy policies breaks down when considering customers interaction with existing privacy policies, users inability to compare privacy policies across competing companies and, most importantly, lock-in situations that prevent users from switching platforms and, increasingly, from switching data ecosystems across devices. Indeed, by specifically framing privacy as a market product, the FTC may have inadvertently given firms who deal in user data the opportunity to consolidate data collection practices and the incentives for more horizontal integration across platforms while paying lip service to privacy protection, as demonstrated by Google’s case earlier in 2012. Pamela Jones Harbour, former FTC Commissioner, noted recently (2012): “Opt out of Google’s data collection? Sure, you can do that—but you’ll also have to delete your Gmail account and leave Google’s ecosystem. With Google’s Android operating system—which is activated in 1.3 million new mobile devices every day, and is used by more people than use Apple’s iPhone—that ecosystem is growing.” Considered from this perspective, it is even questionable whether the notion of “individual choice” can even be used to adequately describe the decision to opt-out of particular data ecosystems: By the time users become concerned about their privacy, they are already locked-in to using particular applications and devices. As Bonneau and Preibusch (2011) conclude

elsewhere, as of last year, there was no market for privacy and no evidence that companies were competing in regard to their privacy policies.

Conclusion: Privacy Remedies for Mobile Ecosystems

In this article, we have used the legal framework of captive audience as a point of departure wherefrom to evaluate the 2012 FTC privacy guidelines. We have argued that central to a captive audience argument is the imbalance of power between communicator and audiences determined by specific contexts of communicative interaction, rather than by the particulars of place or content. Hence, our definition of captive audiences has three components: (a) the extent to which audiences can make autonomous choice about a message; (b) the nature of audiences' expectations of privacy; and (c) availability of functional opt-out mechanisms. We defined functional opt-out mechanisms as means through which audiences are able to exit out of coercive communication situations without significant costs to themselves.

Equipped with these insights, we criticized the 2012 FTC privacy guidelines for falling short of protecting consumers against invasive mobile marketing in at least three respects. First, as mobile marketers' ability to dynamically target individuals based on location, situation, mood, social network, and personal history are rapidly improving, the FTC privacy guidelines ignore how, in the context of data monopolies, the combination of geotagging and data about individuals' personal history threatens individual autonomy and produces situations of compelled persuasion that limit what the Supreme Court called "privacy of choice."

Second, the FTC privacy framework offers guidelines for privacy understood as better control over user's informational choices, but ignores the dimension of privacy that has to do with user's control over communicative interaction. Traditionally, the courts understood this dimension of privacy to be modulated by audiences' differential privacy expectations and

recognize the home as the context of maximum audience choice over communicative engagement. Nothing similar exists in mobile context. Rather, for the mobile environment, a “home” mode with maximum privacy expectations for users may only be achieved by completely turning off their mobile devices or their data networks (which, of course, removes even those communication streams that users would have otherwise allowed in their innermost private circle), or by time-intensive “privacy contract renegotiation” with those marketers otherwise allowed to communicate with the users in regular circumstances. Unless prepared to spend time on adjusting privacy options on a daily basis, users lack the ability to “move in and out of home,” so to say, in mobile context.

Finally, the FTC privacy framework, which continues the tradition of relying on the market and attempts to reframe privacy as a market good to be competed over, does not account for the increasingly large costs that users face when trying to switch among platforms. Indeed, we argue that the Commission’s specific framing of privacy as a product to be competed over may actually offer incentives to companies to use privacy policies as lock-in mechanisms (for example, by horizontal integration and standardization of privacy policies across assets), which may actually increase opt-out costs for consumers, thus diminishing, rather than multiplying, their privacy choices.

In addition to initiatives that the FTC is already working on implementing, such as identifying meaningful privacy disclosures in mobile contexts and discussing ways to standardize mobile privacy policies (e.g., Federal Trade Commission 2012a), privacy scholars have produced a number of recommendations meant to address the imbalance of power between users and marketers in the digital environment. These recommendations include calls for a more active FTC involvement, for example prompts for the FTC to set self-regulation benchmarks

(Turow et al. 2007; Turow 2011) or provide incentive for compliance to privacy standards for online websites by instating a process of periodic review (Park 2011). Among the more creative self-regulatory proposals, Turow (2011) suggests a “Do Not Track” system with rotating “relevance category” that would deliberately mismatch the content of the ad to the identity of the recipient group. This systematic exercise in ad (mis)targeting would presumably educate consumers about the relationship between data collection and content tailoring and would encourage meaningful conversations across social niches.

We agree that consumer privacy education should become a critical component in a modern digital literacies curriculum. With online tracking up 400 percent since 2010 (Farivar 2012), with an estimated one billion mobile customers by 2016 and a mobile spending market of \$1.3 trillion (Panzarino 2012), with technologies being developed by firms such as Drawbridge to track people across all devices and serve them tailored adverts (BBC, 2012), it is imperative that scholars and policy makers examine the nature of the needed digital user competencies able to inform meaningful privacy self-management, and that these competencies become part of the formal curriculum covered in media literacy classes.

However, consumer education alone will not restore the power asymmetries that have tilted decisively in favor of marketers and data-trading companies of the digital marketplace. The captive audience doctrine used in our analysis suggests two rather radical proposals. First, mobile devices should have the ability to negotiate privacy contracts dynamically, without constant user intervention. As Swire (1997) noted early on, under a contractual model of privacy, which the FTC has adopted for the last decade, the market model of privacy fails if consumers have neither the information, nor the bargaining power to negotiate a desired privacy contract. While standardization of privacy policies allows users better insight into what types of data

collection they would otherwise unwittingly agree to, they don't allow the users to renegotiate the privacy contract "on the go" without costly expenditure of attention and time. Thus, standardization of privacy policies should also include users' ability to explore and track, directly from their devices, the list of entities with whom users have already entered into a privacy contract, to classify those entities according to the privacy regime the users wish to grant them, and to automate control of future privacy contracts based on user-specific classifications. Just like the V-chip for television, mobile devices should be equipped with "privacy chips" to control target-specific privacy contract negotiations function of users' preferences.

Second, our analysis also suggests the need for the FTC to define and enforce a "home mode" for the mobile user, a concept akin to the proposal for "digital territories" (Daskala and Maghiros 2006) or "virtual residence" (Hakala and Beslay 2007). Unlike traditional home, the boundaries of the "home mode" would not be marked spatially, but in terms of a dynamic privacy regime that would enables users to tune out marketing communication and data tracking at particular times, while retaining access to the network themselves. As such, the home mode would allow for selective (but not necessarily limited) connectivity within which the individual user control who, how and for what purposes other communicators may reach them.²⁵ In other words, by giving the individual user control over when and to what extent she will be (un)available for informational and communicational flow, the "home mode" would help users bridge the gap between what used to be, in Tavani's (2007) terms, "naturally private" (i.e., the home) and what is normatively private (i.e., the liminal moments regardless of the location).

NOTES

1. *Mainstream Marketing Services, Inc. v. FTC*, 358 F.3d 1228, 1245 (10th Cir. 2004), cert. denied *Mainstream Mktg. Servs. v. FTC*, 543 U.S. 812 (2004).
2. The first ordinance designed to prohibit contact between advertiser and customer unless the contact was specifically allowed by the customer dates back to 1931, to the city of Green River. There, the City responded to complaints by shift workers whose rest was disturbed by the increase in door-to-door selling and passed the Green River Ordinance that prohibited the practice of door-to-door selling unless specifically allowed by a resident (Bene, Lauritzen and McCullers 2007, 9). See also *Town of Green River v. Fuller Brush Co.*, 65 F.2d 112 (10th Cir. 1933).
3. *Public Utilities Commission of the District of Columbia v. Pollak*, 343 U.S. 451, 468 (S. Ct. 1952, J. Douglas dissenting).
4. *Breard v. Alexandria*, 341 U.S. 622 (S. Ct. 1951).
5. *Martin v. Struthers*, 319 U.S. 141 (S. Ct. 1943).
6. *Rowan v. U.S. Post Office Dep't.*, 397 U.S. 728 (S. Ct. 1970); *Mainstream Mktg. Servs. v. FTC*, 358 F.3d 1228 (10th Cir. 2004).
7. *Saia v. New York*, 334 U.S. 558 (S. Ct. 1948); *Kovacs v. Cooper*, 336 U.S. 77 (S. Ct. 1949); *Public Utilities Commission v. Pollak*, 343 U.S. 451 (S. Ct. 1952)
8. *Packer Corp. v. Utah*, 285 U.S. 105 (S. Ct. 1932); *Cohen v. California*, 403 U.S. 15 (S. Ct. 1971); *Erznoznik v. Jacksonville*, 422 U.S. 205 (S. Ct. 1975).
9. *Madsen v. Women's Health Center, Inc.*, 512 U.S. 753 (S. Ct. 1994); *Hill v. Colorado*, 530 U.S. 703 (S. Ct. 2000); *Snyder v. Phelps*, 131 S. Ct. 1207 (S. Ct. 2011).
10. *Frisby v. Schultz*, 487 U.S. 474 (S. Ct. 1988)
11. *FCC v. Pacifica Found.*, 438 U.S. 726 (S. Ct. 1978).
12. *Packer Corp. v. Utah*, 285 U.S. 105, 110 (S. Ct. 1932)
13. *Rosenfeld v. New Jersey*, 408 U.S. 901 (S. Ct. 1972)
14. *Lehman v. City of Shaker Heights*, 418 U.S. 298 (S. Ct. 1974)
15. *Consolidated Edison Co. v. Public Service Commission*, 447 U.S. 530 (S. Ct. 1980)
16. *Saia v. New York*, 334 U.S. 558, 562 (S. Ct. 1948)
17. *Cohen v. California*, 403 U.S. 15, 21 (S. Ct. 1971).
18. See for example *Rowan v. U.S. Post Office Dep't.*, 397 U.S. 728 (S. Ct. 1970), in which the principle that “a man’s home is his castle” is the basis of the ruling.
19. Indeed, as the Supreme Court observed, “a State may permissibly determine that, at least in some precisely delineated areas, a child—like someone in a captive audience—does not possess the capacity for individual choice which is the presupposition of First Amendment guarantees.” *Ginsberg v. New York*, 390 U.S. 629, 649-650 (S. Ct. 1968, Stewart, J., concurring).
20. *Planned Parenthood v. Casey*, 505 U.S. 833, 851 (S. Ct. 1992).
21. David A. J. Richards (1977), for example, connects the right to privacy to the “separateness from other persons” and the ensuing ability to make independent decisions regarding one’s life. Similarly, June A. Eichbaum (1979) argues that the value of privacy as a civil right lies in its ability to protect individual interests, particularly at times when it may conflict with a majoritarian structure.
22. “One important aspect of residential privacy is protection of the unwilling listener. Although in many locations, we expect individuals simply to avoid speech they do not want to hear...the home is different.” *Frisby v. Schultz*, 487 U.S. 474, 484 (S.Ct. 1988).

23. A sign that the household residents do not want to be disturbed is such a signaling mechanism, just like adding one's telephone number to a Do Not Call list. See also (Hartstein 2006, 805), arguing that "...the gravamen of unwilling audience doctrine appears to be the audience's ex ante deliberate and explicit rejection of the expression."

24. For example, a user who happened to start building a movie library using Zune Marketplace service, which utilizes DRM, has only a limited number of Microsoft branded choices for playing the videos on a portable device (e.g., the Zune HD). The remaining portable devices provided by companies will not be able to play the videos (unless the DRM is hacked). Even if the consumer desires to shift to a new video service provider that sells DRM-free videos, the initial library obtained from Zune Marketplace will only be compatible with Microsoft branded portable players, leaving the consumer either with the option of continuing to use Microsoft do away with the library that she owns to move to a new service and a device (or keep both services and carry two portable devices).

25. Tellingly, some commentators called Apple's "Do Not Disturb" mode introduced with iOS 6, a mode which delays phone alerts, "the most thrilling new iPhone feature" (Bosker 2012).

REFERENCES

- Adams, Andrew A, Kiyoshi Murata, and Yohko Orito. 2009. The Japanese sense of information privacy. *AI & Society* 24 (4): 327-341.
- Albert, Lara. 2011. From location-centric to customer-centric. *Direct Marketing News* (May 1). <http://www.dmnews.com/from-location-centric-to-customer-centric/article/201376/> (accessed November 1, 2012).
- Andrejevic, Mark. 2007. *ISpy: Surveillance and power in the interactive era*. University Press of Kansas.
- Balkin, J M. 1999. Free speech and hostile environments. *Columbia Law Review* 99: 2295-2320.
- Baruh, Lemi and Mihaela Popescu. 2010. Behavioral targeting, freedom of speech, and privacy in the age of electronic surveillance: A value-based approach to defining privacy in transnational context. In *Proceedings of the International Conference on New Media and Interactivity Conference (Istanbul, Turkey)*, 219-224.
- BBC, 2012. Tracking adverts set to jump across gadgets. <http://www.bbc.co.uk/news/technology-20638132> (accessed December 20, 2012).
- Bell, Tom W. 1998. Fair use vs. Fared use: The impact of automated rights management on copyright's fair use doctrine. *North Carolina Law Review* 76:557-619.
- Bene, Terry Del, Ruth Lauritzen, and Cyndi McCullers. 2007. *Green River*. Charleston, SC; Chicago, IL; Portsmouth, NH; San Francisco, CA: Arcadia Publishing.
- Benoliel, Daniel. 2004. Technological standards, inc.: Rethinking cyberspace regulatory epistemology. *California Law Review* 92. doi:10.2139/ssrn.1341226.

- Bonneau, J and S Preibusch. 2010. The privacy jungle: On the market for data protection in social networks. In *Economics of Information Security and Privacy*, ed. T. Moore, D. J. Pym and C. Ioannidis, 120-167. New York: Springer.
- Bosker, Bianca. 2012. Do Not Disturb: The most exciting (and underrated) new Apple feature. *The Huffington Post*, June 11. http://www.huffingtonpost.com/bianca-bosker/do-not-disturb-apple-feature_b_1588401.html (accessed June 12, 2012).
- Brownstein, Alan and Vikram David Amar. 2010. Death, grief, and freedom of speech: Does the First Amendment permit protection against the harassment and commandeering of funeral mourners? *Cardozo Law Review De Novo* 368-387.
- Burk, Dan L and Julie E Cohen. 2001. Fair use infrastructure for rights management systems. *Harvard Journal of Law & Technology* 15:41-83.
- Castells, Manuel. 2007. *Mobile communication and society: A global perspective*. Cambridge, Mass.: MIT Press.
- Chellappa, R K and R G Sin. 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management* 6 (2): 181-202.
- Claburn, Thomas. 2011. Google defines social strategy. *Information Week*, May 6. <http://www.informationweek.com/internet/google/google-defines-social-strategy/229403001> (accessed March 15, 2012).
- Cohen, Julie E. 2008. Privacy, visibility, and exposure. *University of Chicago Law Review*, 75: 181-201.
- Corbin, Caroline Mala. 2009. The First Amendment right against compelled listening. *Boston University Law Review* 89:939-1016.

- Daskala, B. and L. Maghiros. 2006. Digital territories. In *2nd IET International Conference on Intelligent Environments*, 221-226.
- Davis, Michael A. 2012. Fundamentals: The mobile payment frontier. InformationWeek Reports, March 26. <http://reports.informationweek.com/abstract/18/8711/Mobility-Wireless/fundamentals-the-mobile-payment-frontier.html> (accessed May 13, 2012)
- DeMartine, Chris. 2011. 2012 outlook: Digital data will take center stage. *Multichannel Merchant*, December 14. <http://multichannelmerchant.com/crosschannel/digital-data-takes-off-1214tpp7/> (accessed March 13, 2012).
- Dick, Alan and Kunal Basu. 1994. Customer loyalty: Toward an integrated conceptual framework. *Journal of the Academy of Marketing Science* 22 (2): 99-113.
<http://dx.doi.org/10.1177/0092070394222001>.
- Duhigg, Charles. 2012. How companies learn your secrets. The New York Times, February 16.
http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0 (accessed May 13, 2012).
- Eichbaum, June Aline. 1979. Towards an autonomy-based theory of constitutional privacy: Beyond the ideology of familial privacy. *Harvard Civil Rights-Civil Liberties Law Review* 14:361-384.
- Ekman, P and W V Friesen. 1969. The repertoire of nonverbal behavior: Categories, origins, usage, and coding. *Semiotica* 1:49-98.
- Farivar, Cyrus. 2012. Online behavioral tracking up 400 percent across prominent websites. *Ars Technica*, June 18. <http://arstechnica.com/business/2012/06/online-behavioral-tracking-up-across-prominent-websites/> (accessed December 19, 2012).

Federal Trade Commission. 2012a. *In Short: Advertising and Privacy Disclosures in a Digital World*.

<http://www.ftc.gov/bcp/workshops/inshort/FinalWorkshopTranscriptAugust72012.pdf>
(accessed August 1, 2012).

———. 2012b. *Protecting Consumer Privacy in An Era of Rapid Change: Recommendations for Businesses and Policymakers*. <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>
(accessed April 12, 2012).

Felten, Ed. 2012. FTC settles with Google over cookie control override. <http://techatftc.wordpress.com/2012/08/09/google/> (accessed December 12, 2012).

Fetscherin, Marc. 2006. Digital rights management: What the consumer wants. *Journal of Digital Asset Management* 2:143-149.

Godwin, Mike. 2004. *What Every Citizen Should Know About DRM, A.k.a. "Digital Rights Management"*. http://www.publicknowledge.org/pdf/citizens_guide_to_drm.pdf
(accessed March 12, 2012).

Goffman, Erving. 1963. *Behavior in public places: Notes on the social organization of gatherings*. New York: Free Press.

Greenhalgh, Andrew. 2008. ICompete: Analyzing vendor-exclusive smartphone tying arrangements under federal law. *Loyola Consumer Law Review* 20:438-476.

Haiman, Franklyn S. 1972. Speech v. privacy: Is there a right not to be spoken to? *Northwestern University Law Review* 67 (2): 153-199.

Hakala, Hannu and Laurent Beslay. 2007. Digital territory: Bubbles. In *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society*, ed. Paul T Kidd, 69-78. Macclesfield: Cheshire Henbury.

- Hall, James A. 1991. The watcher at the gates of dawn: The transformation of self in liminality and by the transcendent function. In *Liminality and Transitional Phenomena*, ed. Nathan Schwartz-Salant and Murray Stein, 33-52. Chiron Publications.
- Hartstein, Daniel E. 2006. Collateral censorship and first amendment theory. *University of Pennsylvania Journal of Labor & Employment Law* 8:765-812.
- Jacobs, Leslie Gielow. 1998. Is there an obligation to listen. *University of Michigan Journal of Law Reform* 32:489-543.
- Jones Harbour, Pamela. 2012. The Emperor of All Identities. *New York Times*, December 18. <http://www.nytimes.com/2012/12/19/opinion/why-google-has-too-much-power-over-your-private-life.html> (accessed December 19, 2012).
- Jung, C. G. 1953. Relations between the ego and the unconscious. Vol. 22 of *The Collected Works of C. G. Jung*, ed. Michael Fordham, Gerhard Adler, and Herbert Read. New York: Pantheon Books.
- Kelley, P G, J Bresee, L F Cranor, and R W Reeder. 2009. A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1-12.
- Kelley, P G, L Cesca, J Bresee, and L F Cranor. 2010. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, 1573-1582.
- Klaassen, Abbey and Kunur Patel. 2009. Places, please: Location changes digital marketing. *Advertising Age*, September.
- Lederman, Anne D. 1995. Free choice and the First Amendment or would you read this if I held it in your face and refused to leave? *Case Western Reserve Law Review* 45:1287-1323.

- Lessig, Lawrence. 2004. *Free culture: How big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press.
- Lievrouw, Leah A and Sonia M Livingstone. 2002. Introduction. In *Handbook of New Media: Social Shaping and Consequences of ICTs*, 1-15. London ; Thousand Oaks Calif.: SAGE.
- Marcus, Joshua. 1998. Commercial speech on the internet: Spam and the First Amendment. *Cardozo Arts and Entertainment Law Journal* 16:245-302.
- Marx, Gary T. 2001. Murky conceptual waters the public and the private. *Ethics and Information Technology* 3 (3): 157-169.
- McDonald, Aleecia M., Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. A comparative study of online privacy policies and formats. In *Privacy Enhancing Technologies*, ed. Ian Goldberg and Mikhail J. Atallah, 37-55. Berlin; Heidelberg: Springer.
- McGee, Thorin. 2011. The Big Qs of 2011. *Target Marketing*, January.
- Nagel, Thomas. 1998. Concealment and exposure. *Philosophy and Public Affairs* 27 (1): 3-30.
- Nissenbaum, Helen. 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
- Panzarino, Matthew. 2012. Forrester: 1B smartphone and tablet users by 2016, with Apple, Google and Microsoft powering 90%, *The Next Web*, February 13, <http://thenextweb.com/mobile/2012/02/13/forrester-1b-smartphone-users-by-2016-with-apple-google-and-microsoft-powering-90/> (accessed December 20, 2012).
- Park, Yong Jin. 2011. Provision of internet privacy and market conditions: An empirical analysis. *Telecommunications Policy* 35 (7): 650-662.

- Preibusch, S and J Bonneau. 2011. The privacy landscape: Product differentiation on data collection. In *The Tenth Workshop on the Economics of Information Security (WEIS)*, http://www.cl.cam.ac.uk/~jcb82/doc/PB11-WEIS-privacy_landscape.pdf (accessed September 26, 2012).
- Prosser, William L. 1960. Privacy. *California Law Review* 48 (3): 383-423.
- Richards, David A J. 1977. Taking "taking rights seriously" seriously: Reflections on dworkin and the american revival of natural law. *New York University Law Review* 52 (6): 1265-1340.
- Schiller, Dan. 2007. *How to think about information*. Urbana: University of Illinois Press.
- Shapiro, Carl and Hal R Varian. 1999. *Information rules: A strategic guide to the network economy*. Boston, Mass.: Harvard Business School Press.
- Shapiro, Stuart. 2006. Places and spaces: The historical interaction of technology, home, and privacy. *The Information Society* 14 (4): 275-284.
- Sheller, Mimi and John Urry. 2003. Mobile transformations of 'public' and 'private' life. *Theory, Culture & Society* 20 (3): 107-125.
- Shin, Dong-Hee and Won-Yong Kim. 2008. Forecasting customer switching intention in mobile service: An exploratory study of predictive factors in mobile number portability. *Technological Forecasting and Social Change* 75 (6): 854-874.
- Silva, Adriana de Souza e and Jordan Frith. 2012. *Mobile interfaces in public spaces*. New York; London: Routledge.
- Strandburg, Katherine H. 2011. Home, home on the web and other Fourth Amendment implications of technosocial change. *Maryland Law Review*, 70: 614-680.

- Swire, P. 1997. Markets, self-regulation, and government enforcement in the protection of personal information, in privacy and self-regulation in the information age by the US department of commerce. In *Privacy and Self-Regulation in the Information Age*. Ed. US Department of Commerce. <http://www.ntia.doc.gov/print/page/chapter-1-theory-markets-and-privacy>.
- Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1–22.
- The Toronto Star*. 2012. How U.S. consumers benefit from Ontario Privacy Chief; Cavoukian's philosophy of “privacy by design” gaining currency. March 3.
- Turner, Victor W. 1967. *The forest of symbols: Aspects of Ndembu ritual*. Ithaca, N.Y.,: Cornell University Press.
- . 1969. *The ritual process: Structure and anti-structure*. Chicago,.
- . 1974. *Dramas, fields, and metaphors: Symbolic action in human society*. Ithaca N.Y.: Cornell University Press.
- Turow, J., C J Hoofnagle, D K Mulligan, and N Good. 2007. The Federal Trade Commission and consumer privacy in the coming decade. *I/S: A Journal of Law and Policy for the Information Society* 3: ISJLP 3:723-749.
- Turow, Joseph. 2011. *The Daily You: How the new advertising industry is defining your identity and your world*. New Haven: Yale University Press.
- van Gennep, Arnold. 1909. *Les rites de passage; Étude systématique des rites de la porte et du seuil, de l'hospitalité, de L'adoption, de la grossesse et de l'accouchement, de la naissance, de l'enfance, de la puberté, de l'initiation, de l'ordination, du couronnement des fiançailles et du mariage, des funérailles, des saisons, etc.* Paris: É. Nourry.

Zarsky, Tal Z. 2004. Desperately seeking solutions": Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society.

Maine Law Review 56 (1): 13-59.

Zick, Timothy. 2007. Clouds, cameras, and computers: The First Amendment and networked public places. *Florida Law Review* 59:1-69.