Surveillance & Society

Debate

Caveat Emptor:
A Perspective on Consumer Privacy Online

Stephen T. Margulis

Grand Valley State University, USA. margulis@gvsu.edu

Gary T. Marx

MIT, USA. gtmarx@mit.edu

In light of the hyperbole—and even hysteria in some circles—over an approaching privacy cliff and the informative and critical attention to privacy this journal has previously paid[1] with respect to issues such as how privacy is light on being a social rather than only an individual value; how it can encourage an ad hoc, jerry-rigged technology-specific approach, rather than one grounded in a comprehensive theory of personality and human dignity; its tendency to slight questions of justice and fairness at the altar of individualism and property; and its tilt away from an equally important and terribly neglected question of publicity (with its obligations and rights to reveal, as well as protect information) (Marx 2011), we might be excused for bringing less than overflowing enthusiasm to yet another discussion of privacy. However, as Colin Bennett (2011) wisely notes, given our culture and popular understandings, it is likely the best term we have for public communication of the issues. That is certainly the case for online privacy with respect to consumer concerns—the topic we will discuss. Rather than dealing with the clouds of abstraction, strong advocacy of a normative position, or prognostication, we ask, "what are some of the findings of social science research for consumer's online privacy concerns?"

Online commerce is big business and is expected to grow. In the U.S. in 2011, consumers spent about $200 billion online (www.internetretailer.com/trent/sales). A major factor that differentiates online from most offline conditions is the collection, retention, distribution, merging and use of personal information by online businesses and information brokers. Online companies claim that information collection allows them to personalize products and services to their customers and, by creating loyal customers, companies benefit (Culnan and Bies 2003). However, the benefits of personalization do not override privacy concerns for most consumers (Han and Maclaurin 2002). In fact, according to polling data, consumers have real privacy concerns about their personal information online (see www.truste.com/about-TRUSTe/press-room/news_truste_releases-us_customer_findings_report and www.webpronews.com/seriously-for-the-last-time-nobody-likes-being-tracked-online-2012-04 for 2012 polls). Unfortunately, too many online businesses fail to effectively address consumers' privacy concerns (discussed below).

Privacy and trust are variables that predict online purchasing and purchasing intentions (e.g. Smith, Dinev and Xu 2011). However, privacy is an elusive concept (see e.g. Smith et al. 2011). Nevertheless, certain elements are common to a number of definitions: control over transactions between person(s) and other(s) and the goals of enhancing autonomy and/or minimizing vulnerability (Margulis 2003). Different interpretations of these elements and the inclusion of additional variables generate a variety of definitions of privacy, such as those found in many consumer online privacy studies. Common elements in definitions of trust are awareness of one's vulnerability to harm by other(s) and a belief in the positive intentions of

[1] e.g. the debate initiated by Colin Bennett (2011) in *Surveillance & Society* 8(4), http://www.surveillance-and-society.org/ojs/index.php/journal/article/downloadSuppFile/privacy_defence/privacy_debate

Margulis, S.T. and G.T. Marx. 2012. Caveat Emptor: A Perspective on Consumer Privacy Online. *Surveillance & Society* 10(3/4): 351-355. http://www.surveillance-and-society.org | ISSN: 1477-7487

the other(s) toward one's self (Fulmer and Gelfand 2012). A shared element, vulnerability, links privacy and trust. Vulnerability underlies consumers' online privacy concern. Though studies agree that privacy and trust are related (e.g. Smith et al. 2011), there is no consensus on the nature of the relationship.

Although studies hypothesize that low privacy concerns and/or high trust in a website are antecedents of online behaviors, such as protective behaviors (e.g. Milne, Labrecque and Cromer 2009), relatively few studies have directly examined the influence of privacy and trust specifically on online purchasing decisions and intentions (see Smith et al. 2011 for a review). Most of those studies support that relationship (e.g. Milne and Boza 1999; Ranganathan 2012). However, the relationship is often influenced/moderated by additional factors, such as familiarity with an e-tailer (Van Slyke, Shim, Johnson and Jiang 2006).

Building trust is more effective (on average) than reducing privacy concerns for gaining competitive advantage (Milne and Boza 1999). Researchers have posed a number of ways to build trust. We address consumer trust and consumer privacy concerns by focusing on what Svenonius (2010) calls the "consumer rights regime": the role of "legislation, consumer organizations and protection agencies, and mediation boards" on creating trust (2010: 313).

The U.S. Federal Trade Commission (FTC), a consumer protection agency, advocates five fair information practice principles (FIPPs) to address consumer privacy concerns. In brief, they are: notice of information practices; consumer choice on how personal information is used beyond its intended use; reasonable access to one's personal information at a website and the ability to ensure its accuracy and completeness; the taking of reasonable steps to ensure the security of personal information at a website; and instituting an enforcement mechanism through self-regulation, enforceable regulations, or legislation (www.ftc.gov/reports/privacy3/fairinfo.shtm). The FTC has proposed a new privacy framework, based on best practices, that subsumes the five FIPPs and also addresses reasonable information collection limits, sound retention practices, and consumer education about commercial data privacy practices (FTC 2012).

Culnan and Bies (2003) argue that a company's use of FIPPs addresses fairness by providing consumers with control and voice with regard to disclosures and by signaling that a firm can be trusted with disclosed information.[2] If e-tailers were to fully implement FIPPs via privacy notices and supporting policies and procedures, consumers should have far fewer major privacy concerns. However, currently, the FTC's FIPPs are not legally required because the FTC failed to get supporting legislation for this policy.[3] To extend its legal reach, because many companies, online and offline, have failed to effectively implement the five FIPPs (see below), the FTC again has called for supporting legislation to put legal bite in its new framework.

However, from Congress' perspective, self-regulation by online firms, if it was consumer responsive, would probably make legislation unnecessary (Culnan and Bies 2003). But just how effective online self-regulation has been for consumers is an open question. Several studies report that most companies' privacy policies do not include all the FIPPs (e.g. Sheehan 2005). Moreover, many privacy policies are not understandable (Culnan and Bies 2003). Their purpose is too often to reduce the company's liability, not to protect the consumer (e.g. Papacharissi and Fernback 2005). Although consumers prefer websites with privacy notices over those without them (Pan and Zinkhan 2006), only about 30 per cent of consumers closely read a website's privacy policies (Consumer Awareness Project 2009 at www.cdt.org/privacy/guide/surveyinfo.php; also see Milne and Culnan 2004). We are left to wonder whether the FTC's new framework will be any more successful than its five FIPPS if it lacks legislative support.

[2] Currently, there is no consensus on the nature of the relationship between fairness and trust.
[3] Only if a firm's business practices are deceptive or fraudulent can the FTC can take legal steps.

Moreover, because the U.S. views privacy as a relative, not an absolute, right, Congress has resisted general consumer privacy legislation in favor of limited sectoral legislation, e.g. protection for children online and of video rental, medical and financial records (see e.g. Langenderfer and Miyazaki 2009). For example, three general privacy bills, and a fourth aimed at children and teens, plus eight bills addressing data security and data breach notification (FTC 2012: notes 16, 18 and 19) have languished in the current (112th) Congress. One explanation of Congressional resistance is that such legislation has the potential to increase the cost of conducting business, hence lowering profits—a particular concern to low-margin companies (Smith et al. 2011). Regan (1995) provides another explanation. Framing privacy as an individual right (interest) has had a weak impact on congressional policy-making because it enables groups that would bear the costs of the proposed privacy legislation to eventually shape or undermine the privacy legislation by asking that individual privacy interests be balanced with presumably higher interests that serve the public good, such as organizational efficiency and business competitiveness. In this regard, polls on privacy concerns seem to focus on privacy as an individual good, not a public good. That most consumers have moderate, not high, privacy concerns (Sheehan 2002) is potentially another basis for resisting legislation. If consumer privacy legislation is to be enacted, Culnan and Bies (2003) argue what we should expect is sectoral legislation, a convergence of business and consumer interests, and strong media attention to the issue. Might opinion polls on consumers' privacy concerns stimulate legislation? That's uncertain. Gandy (2003) argues that because private corporations are the primary sponsors of privacy polls, these polls and their authors have nudged the policy debate toward self-regulation as the answer. All of these factors work against Congress passing strong consumer privacy legislation.

There are some organizational bases for increasing trust and reducing privacy concerns. One example is the third-party guarantor, such as TRUSTe. TRUSTe provides its clients—commercial websites—with a privacy seal of approval "suited to [its] business practices" and compliant with "federal and state requirements" (www.truste.com). Operationally, the seal addresses two FIPPs: notice and choice. (www.truste.com). Privacy seals are associated with greater trust in a website and a more favorable attitude toward the company's privacy policies (see e.g. Miyazaki and Krishnamurthy 2002). Also, a commercial website's reputation can increase a consumer's trust in a website (see Li 2011 for a review). In this regard, some websites provide reputational indicators of vendor trustworthiness, such as eBay (using consumer feedback on online sellers) and Angie's List (using consumer feedback on offline service providers).

TRUSTe reports that its seals positively impact consumer purchasing. Unfortunately, other studies report that a privacy seal does not necessarily means better privacy practices or the collection of less personal information (see Smith et al. 2011 for a review).[4] Moreover, a study of online advertising found that only those consumers who had both prior negative attitudes toward advertising and a high desire for privacy had more positive purchase intentions because of privacy seals (Stanaland, Lwin and Miyazaki 2011). Finally, a privacy seal is no guarantee that a website is free of malware or spam. One study found a higher rate of malware and/or spam at websites with a TRUSTe privacy seal than those without it (www.benedelman.org/news/092506-1.html).

In the absence of legislative or regulatory or reputational protection, a potential protection for a consumer with a grievance against an e-tailer is alternative dispute resolution (ADR), the threat of which might deter bad practices or at least offer some redress to those wrongly treated. The most common form employed by offline companies is binding arbitration. Among its disadvantages to consumers are its potential to be expensive and that the vendor might choose an arbitrator who has favored the vendor in the past. (http://www.nolo.com/legal-encyclopedia/arbitration-clauses-contracts-32644.html). By comparison, mediation is common in Europe (Svenonius 2010). In this regard, TRUSTe will mediate online, eligible

[4] There is also a threat posed by websites that "copy and paste" a legitimate privacy seal onto their own website, presumably a deceptive practice that the FTC could investigate.

privacy complaints of consumers against client websites without cost to the consumer. TRUSTe's determination is not legally binding on the consumer (unlike binding arbitration) but it is binding on the website. Moreover, consumers can appeal decisions and TRUSTe punishes uncooperative websites (http://www.truste.com/products-and-services/dispute-resolution-services/dispute-resolution-faq). What is needed is research on websites' use of ADR: its forms, their frequency, and consumers' judgments of ADR's efficacy, trustworthiness, and fairness.

Another potential contribution to addressing consumer concerns involves Privacy Impact Assessments (PIA). Wright and de Hert (2012) and colleagues from several disciplines have critically analyzed this emerging privacy tool. The policy tries to anticipate problems, seeking to prevent, rather than to put out, fires. The PIA model is adopted *before* personal data practices are established. It involves a variety of stakeholders and tries to learn from the past and to imagine how new technologies and practices might bring new problems—including that intriguing class of the "unknown unknowns." Marx (2012) offers a critical analysis of the tool and calls for conceptual elaboration with respect to the kinds of privacy problems that appear and the stage of the surveillance process or cycle where they appear. PIA is very much a work in development but offers a model for raising awareness and for trying to bring some balance to conflicting interests. On the other hand the practice is voluntary. Thus, in the final analysis, and consistent with American political economy, we conclude *caveat emptor.*

References

Bennett, C. 2011. In defence of privacy. *Surveillance & Society* 8(4): 485-496.

Culnan, M. J. and R. J. Bies. 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues* 59(2): 323-32.

FTC. 2012. *Protecting consumer privacy in an era of rapid change: Recommendations to businesses and policymaker*. Washington, DC: Federal Trade Commission.

Fulmer, C. A. and M. J. Gelfand. 2012. At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management* 38(4): 1167-1230.

Gandy, O. H., Jr. 2003. Public opinion surveys and the formation of privacy policy. *Journal of Social Issues* 59(2): 283-300.

Han, P. and A. Maclaurin. 2002. Do consumers really care about online privacy? *Marketing Management* 11(1): 35-38.

Langenderfer, J. and A. D. Miyazaki. 2009. Privacy in the information economy. *Journal of Consumer Affairs* 43(3): 380-388.

Li, Y. 2011. Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems* 28(1).

Margulis, S. T. 2003. Privacy as a social issue and a behavioral concept. *Journal of Social Issues* 59(2): 243-262.

Marx, G.T. 2011. Turtles, firewalls, scarlett letters and vacuum cleaners: Rules about personal information. In *Making Privacy*, eds W. Aspray and P. Doty, 271-294. Latham, MD: Scarecrow Press.

——— . 2012. Foreword: Privacy is not quite like the weather. In: *Privacy Impact Assessment*, eds H. Wright and P. de Hert. New York: Springer.

Milne, G. R. and M.-E. Boza. 1999. Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing* 13(1): 5-24.

Milne, G. R. and M. J. Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing* 18(3): 15-29.

Milne, G. R., L. I. Labrecque and C. Cromer. 2009. Toward an understanding of the online customer's risky behavior and protection practices. *Journal of Consumer Affairs* 43(3): 449- 473.

Miyazaki, A. D. and S. Krishnamurthy. 2002. Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs* 36(1): 28-49.

Pan, Y. and G. M. Zinkhan. 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing* 82(4): 331-338.

Papacharissi, Z. and J. Fernback. 2005. Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting and Electronic Media* 49(3): 259-281.

Ranganathan, C. 2012. The role of extrinsic cues in consumer decision process in online shopping environments. *Journal of Electronic Commerce in Organizations* 10(1): 52-71.

Regan, P. M. 1995. *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, NC: University of North Carolina Press.

Sheehan, K. B. 2002. Toward a typology of internet users and online privacy concerns. *The Information Society* 18: 21-32.

——— . 2005. In poor health: An assessment of privacy policies at direct-to-consumer websites. *Journal of Public Policy and Marketing* 24(2): 273-283.

Smith, H. J., T. Dinev and H. Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35(4): 989-1015.

Stanaland, A., M. Lwin and A. Miyazaki. 2011. Online privacy trustmarks: Enhancing the perceived ethics of digital advertising. *Journal of Advertising Research* 51(3): 511-523.

Svenonius, O. 2010. Exploring consumer rights regimes and internet consumption in Europe. In: *Surveillance, privacy, and the globalization of personal information: International comparisons* , eds E. Zuriek, L. L. Harling Stalker, E. Smith, D. Lyon and Y. E. Chan, 310-327. Montreal and Kingston: McGill-Queen's University Press.

Van Slyke, C., J. T. Shim, R. Johnson and J. Jiang. 2006. Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems* 7(6): 415-444.

Wright, H. and P. de Hert. 2012. *Privacy Impact Assessment.* New York: Springer.