The Challenge of Online Privacy to Global Marketers

Héctor R. Lozada
Seton Hall University

Gary H. Kritz
Seton Hall University

Alma Mintu-Wimsatt
Texas A & M University-Commerce

Over the past year the debate on the challenges that online privacy pose to global marketers has intensified. As a result, there is a push in the U.S. and the European Union to protect consumer online privacy and this push is being countered by a move by online advertisers and marketers to self-regulate. In this article, the authors outline tactics that marketers pursue that have come under serious scrutiny over the past two years. Also addressed are legal and voluntary measures that are being considered, and recent infractions that are cause for concern. The article concludes by addressing areas that remain unclear regarding privacy protection and consumer trust.

INTRODUCTION

As of March 2012, twenty countries, including China, the United States and Russia, account for 75 percent of world Internet users, while the remaining 25 percent of Internet use is shared by 226 countries (Internet World Statistics, 2012). Fifty eight countries (16 percent of the world's population) have Internet penetration rates of fifty percent or more of their population, and when added they account for about 72 percent of world Internet users (Internet World Statistics, 2012a). With only about 40 percent of its population having access to the Internet, China still represents the largest world user, followed by the United States.

The Internet has enabled us to change and expand the way we communicate with one another, doing away with some geographical and time barriers. More importantly, it has changed the way we access information and expand our knowledge. Through the Internet, businesses can sell and communicate with customers. The Internet also allows businesses to identify and learn about their customer base. In summary, the Internet has had a definite impact on the way consumers and business organizations relate to one another, globally.

With acceptance, though, comes a decrease in skepticism. Consumers may assume that the same laws or societal rules that protect privacy in the physical world apply to the digital world as well. Contrary to this assumption, the Internet remains largely unregulated and the policies governing it underdeveloped (Privacy Rights Clearinghouse, 2012). Laws concerning online privacy are still being developed. The U.S. Supreme Court largely has taken a hands-off approach to regulating the Internet and online privacy

in favor of free speech. However, the federal government is increasingly interested in regulating the Internet, for example through child pornography and gambling laws (Hunter, Lozada, & Mayo 2010).

Presently there is impetus for the creation of government regulation in the U.S. and abroad as business organizations operating in a global environment rely more heavily on the Internet and on new media for initiating, facilitating and maintaining contacts with customers. Our goal here is to continue the discussion on online privacy, with a focus on highlighting some of the issues that have intensified over the past couple of years.

ONLINE PRIVACY: HOW INFORMATION ABOUT CUSTOMERS FLOW SOMEWHAT FREELY TO MARKETERS

Lohr (2010) asserts that while individuals would not consider giving a stranger their social security number or their email address, they often dole out all kinds of personal information on the Internet that allows such identifying data to be deduced. Internet users provide information to others at almost every step of an online session. Frequently, this information is like a puzzle that needs to be connected before the user's picture is revealed (Privacy Rights Clearinghouse, 2012). The following Internet activities reveal user information: signing up for Internet service, e-mail and list-serves, browsing the Internet, instant messages and social networks (interactive use), personal Web sites and blogs, managing your financial accounts and online bill payments. Users often do not realize that information they provide to one person or company may not make sense unless it is combined with information they provide to another person or company.

E-mail

One of the most basic and frequently engaged online activities involves using e-mail. When a person corresponds through e-mail, they obviously realize that they are giving information to the recipient. What the initiator of the message may not realize is that he/she might also be giving information to any number of people, including their employer, the government, their e-mail provider, and anybody that the recipient passes the message to. In the U.S., the federal Electronic Communications Privacy Act (ECPA) makes it unlawful under certain circumstances for someone to read or disclose the contents of an electronic communication (US Department of Justice, 2010). The ECPA, however, contains many exceptions. For example, the ECPA makes a distinction between messages in transit and those stored on computers, with stored messages generally given less protection than those intercepted during transmission. Additionally, if the e-mail system is owned by an employer, the employer may inspect the contents of employee e-mail on the system, and is therefore not private.

Web Browsing and Cookies

From our standpoint as marketers, perhaps the most relevant consumer online activity is Web browsing. When users visit different Web sites, many of the sites deposit data about their visit on their hard drive. Cookies, as they are known, are pieces of information sent by a Web server to a user's browser. They may include information such as login or registration identification, user preferences, and online shopping cart information. The browser saves the information, and sends it back to the Web server whenever the browser returns to the Web site. For marketers, cookies are extremely useful since they allow the Web server to customize the display it sends to the user, or it may keep track of the different pages within the site that the user accesses. Take as an example a registration card for a product that a customer fills out online. The customer generally provides name and address, which is then stored in a cookie. The marketer then uses cookies to make special offers to returning users and to track the results of their advertising. Some users may be well aware of these so-called first-party cookies. What they may not know is that there are some cookies (third-party cookies) that communicate data about the user to an advertising clearinghouse which in turn shares that data with other online marketers. Additionally, users may not be aware that many websites have begun to utilize a new type of cookie called a *flash cookie* that is more persistent than a regular cookie (Privacy Clearing House, 2012). Flash cookies may carry on

despite user efforts to delete all cookies. Among the companies using flash cookies are MySpace, ABC, ESPN, Hulu, MTV, NBC Universal, Disney, and Warner Brothers. Between July and September 2010 least five class-action lawsuits were filed in California accusing these media companies and technology companies like Specific Media and Quantcast of surreptitiously using flash cookies. According to Vega (2010), the lawsuits contend that the companies collected information on the Web sites that users accessed and from the videos they watched, even though the users had set their Web browser privacy settings to reject cookies that could track them. Scott A. Kamber, a privacy and technology lawyer with KamberLaw who is involved with some of the cases states that these cases are about the right of a computer user to dictate the terms by which their personal information is harvested and shared (in Vega, 2010). These cases are still pending at the time of this writing.

Web Bugs

Many Web sites use Web bugs to track who is viewing their pages. A Web bug (also known as a tracking bug, pixel tag, Web beacon, or clear gif) is a graphic in a Web site or a graphic-enabled e-mail message (Privacy Rights Clearinghouse, 2012). The Web bug can confirm when the message or Web page is viewed and record the IP address of the viewer. Regrettably, users have little control over the data collection by Web bugs on most sites. Furthermore, Web bugs placed by third-parties are not governed by a website's privacy policy.

Direct Marketing

Consumers may notice that online newspapers and other businesses have boxes asking if the website can save their account information for future transactions. Unbeknown to most, though, whether it asks for permission to save a person's information or not, that information is being stored and used by the marketing department. In this context, direct marketing is a sales pitch targeted to a person based on prior consumer choices (Privacy Rights Clearinghouse, 2012). This is how Amazon.com may recommend books that are similar to others that have been purchased by a customer, or how Google's e-mail service, Gmail, places relevant advertisements next to e-mail by scanning incoming e-mails.

Behavioral Marketing or Targeting

Behavioral marketing or targeting refers to the practice of collecting and compiling a record of individuals' online activities, interests, preferences, and/or communications over time. Companies engaged in behavioral targeting routinely monitor individuals, the searches they make, the Web pages they visit, the content they view, their interactions on social networking sites, the content of their emails, and the products and services they purchase. Further, when consumers are using mobile devices, even their physical location may be tracked. This data may be compiled, analyzed, and combined with information from offline sources to create even more detailed profiles.

Marketers can then use this information to serve advertisements to a consumer based on his or her behavioral record. Ads may be displayed based upon an individual's web-browsing behavior, such as the pages they have accessed or the searches they have made. Advertisers believe that this may help them deliver their online advertisements to the users who are most likely to be influenced by them. Behavioral information can be used on its own or in conjunction with other forms of targeting based on factors like geography or demographics. Marketers have developed an array of sophisticated data collection and profiling tools which monitor and analyze our online activity. Typically, behavioral targeting will place a cookie on the user's computer. The cookie might link the user to categories based on the content of the pages they visit. The cookie can then be used to show people ads that are relevant to their interests, regardless of the sites they are visiting. Google, Microsoft, and Yahoo all engage in some form of behavioral targeting.

Vega and Kopytoff (2010) assert that behavioral targeting as a tool has grown enormously over the past decade. As an example, they cite an analysis of ad agency data by The Interactive Advertising Bureau that found that in 2009, 80 percent or more of digital advertising campaigns incorporated behavioral targeting in some way (Vega & Kopytoff, 2010). Moreover, PricewaterhouseCoopers claims

that online advertising revenue, including contextual and behavioral ads, was $12.1 billion for the first half of 2010, an 11.3 percent increase over the same period last year. Google representatives say they expect display ads to become a $50 billion market by 2015 (Vega & Kopytoff 2010).

CHALLENGES OF ONLINE PRIVACY TO GLOBAL MARKETERS

Online Privacy Laws

According to Miyazaki (2008), a major concern with online privacy involves how cookies are placed on the Internet user's hard drive by a third party not directly visited by the online consumer. These "third-party cookies" are often sanctioned by the visited Web site to build consumer profiles by the third party organization for targeted marketing purposes (Lavin, 2006; Raghu, Rao, & Whinston, 2001). Third-party cookies have been a concern of the FTC since 2000. The FTC examined Web sites and found that 57% of sites in a random-sample group (N=335) and 78% of the busiest U.S. sites (N = 91 of the 100 busiest sites) allowed cookie placement by third parties. Another concern is the covert usage of these cookies. The placement of third-party cookies is often facilitated by the use of "clear GIFs" that are only one pixel by one pixel in size, which essentially makes them invisible to the consumer (Hoofnagle, 2005; Martin, Wu, & Alsaid, 2003; Miyazaki, 2008). The FTC (2000) described cookies as a "nonobvious" means of information collection and their undisclosed use as a clear violation of the notice aspect of fair information practices.

To some advertising and media experts, explaining the technology behind the ads might not be a worthwhile means of allaying the fears of consumers who worry about being tracked or who simply fear that someone they share a computer with will see what items they have browsed (Helft & Vega, 2010).

Despite all of the above, there have not been many studies that have examined consumers' willingness to provide personal information and whether or not they are aware of how the information is being used and collected in an online context since around the year 2000. Sheehan and Hoy (2000) suggested that consumers' concerns about privacy are much less when they are familiar with the company asking for the information (an issue of exchange), the type of information being asked for, and whether or not the individual has a relationship with the company. Phelps, Nowak, and Ferrell (2000) indicate that consumers are least willing to provide financial and personal identifier information. They also say that consumers should be provided with at least some control or input into the subsequent dissemination of personal information. But although the FTC's past goal in 1999 and 2000 was to encourage industry self-regulation, the FTC also stated that further improvement was required to protect the privacy of online consumers effectively. That has not happened. The online technology of company information gathering software has increased dramatically in the last twelve years, and the concerns of the government and the consumer have reached epic levels. Fueling these concerns were information leaks and scandals along with the development and popularity of social media networks and websites that blurred the lines of privacy.

Considering how much information we entrust to the Internet every day, it is hard to believe there is no general law to protect people's privacy online. Companies harvest data about people as they surf the Net, assemble it into detailed profiles and sell it to advertisers or others without ever asking permission. In March, 2011, President Obama called for legislation in response to the growing global movement to protect consumers' privacy information online. Microsoft said it supports a broad-based privacy law and, for the time being, introduced a version of its Explorer browser that allows surfers to block some tools advertisers use to track consumers' activities online. By April 2011, Senators John McCain and John Kerry introduced a privacy bill entitled "The Commercial Privacy Bill of Rights" (Kerry, 2011). Lee (2011), it was a legislative move that was designed to centralize various privacy efforts already under way from industry trade groups, government regulators and the Obama administration. To Senator Kerry (2011a), the Commercial Privacy Bill of Rights will establish a baseline code of conduct for how personally identifiable information and information that can uniquely identify an individual or networked device are used, stored, and distributed. The main intent of this legislation would be to increase consumer

trust in the market and to protect people from unscrupulous actors in the market by creating a set of basic rights to which all Americans are entitled" (Kerry, 2011a).

New Jersey became in 2008 the first court in the nation to rule that people have an expectation of privacy when online (Hester, 2008). When ruling in state cases, this new ruling will take precedent of the much weaker Supreme Court decisions stating there is no privacy on the internet (Hester, 2008). This ruling was handed down in a case involving federal officials seeking a user's private information during the investigation of a crime involving her computer. The seven-member court ruled that federal officials do have a right to a user's information when investigating a crime but they must follow legal procedures, securing a grand jury warrant first. Grayson Barber, a Trenton-based lawyer arguing for privacy groups explained that "people use the internet much like the phone making personal and sometimes sensitive transactions they don't believe police will be able to access" (Hester, 2008). The court's ruling, "We now hold that citizens have a reasonable expectation of privacy protected by Article I ... of the New Jersey Constitution, in the subscriber information they provide to Internet service providers -- just as New Jersey citizens have a privacy interest in their bank records stored by banks and telephone billing records kept by phone companies" (Hester, 2008) seems to lend itself to a broader interpretation. New Jersey's ruling means that the court interprets New Jersey's constitution to say that ordinary state citizens have a fundamental expectation of privacy when online.

In the European Union, the Data Protection Act of 1998 (DPA) implemented a European Directive to introduce privacy rights into domestic law. In April 2011, EU justice commissioner, Viviane Reding, announced plans to modernize data protection laws to increase the burden on those handling personal information (Butterworth & Bowcott, 2011). Commissioner Reding's proposal is of "privacy by default," therefore outlawing the current practice of requiring users of social networking and other sites to opt for privacy (opt out of data collection). A "privacy by default" rule would require explicit consent for private information such as email addresses, retained for one reason, to be used for another, and would prevent the collection of irrelevant data through software applications. Ms. Reding also wants services aimed at EU users to be bound by the EU's data protection laws regardless of their location (Butterworth & Bowcott, 2011).

Self-Regulation: Opt Out of Behavioral Targeting

The Commercial Privacy Bill of Rights (Kerry, 2011) would require collectors of information to provide clear notice to individuals on the collection practices and the purpose for such collection. Furthermore, the collector must provide the ability for an individual to *opt out* of any information collection that is unauthorized by the Act and provide affirmative consent (opt in) for the collection of sensitive personally identifiable information. Respecting companies existing relationships with customers and the ability to develop a relationship with a potential customers, the bill would require robust and clear notice to an individual of his or her ability to opt-out of the collection of information for the purpose of transferring it to third parties for behavioral advertising. It would also require collectors to provide individuals either the ability to access and correct their information, or to request cessation of its use and distribution.

The Network Advertising Initiative (NAI) is a cooperative of online marketing and analytics companies committed to building consumer awareness and establishing responsible business and data management practices and standards (NAI, 2010). As increasingly sophisticated online advertising technologies evolve, consumer concerns about their impact on online privacy mount. The NAI is prepared to meet these concerns with both effective industry self-regulation and sensible protections for online consumers. The NAI Opt-out Tool was developed in conjunction with our members for the express purpose of allowing consumers to "opt out" of the behavioral advertising delivered by their member companies.

Recent Violations to Consumers' Online Privacy

Even Apple, who boasts superior security in its products, was susceptible to an attack via one of its Internet service provider, re-emphasizing concerns over privacy. When it introduced the iPad in late

April, 2010, the company did not contemplate that by early June, 2010, they would be dealing with a hacking incident in which prominent users of its new iPad 3G, including military and government officials as well as media personalities and celebrities, had their e-mail addresses hacked by a group that shared its findings with online publication Valleywag to point out security flaws in AT&T's Web servers (Choney, 2010).

On November 3, 2010 Facebook announced new features that will allow local merchants and retailers to offer coupons and specials through its mobile application to U.S. users (for now) who check in to their place on Facebook (Fougner, 2010). This is quite interesting, given that a few weeks prior, Facebook acknowledged that some applications on its site had improperly shared identifying information about users and, in some cases, their friends, with advertisers and Web tracking companies (Helft, 2010). The company vowed to fix the problem and be more vigilant, although they also played down the importance of this leak. Please note that two days prior to Facebook's announcement introducing deals, Twitter started dropping advertisements into individual users' streams (Lee, 2010). These paid advertisements appear in a user's Twitter stream regardless of whether they follow that advertiser or search for anything on Twitter.

In September 2011, European regulators pressed Google, to change the way it collects data on cellphone locations worldwide (O'Brien, 2011). In this regard, European regulators appear to be baffled by the tracking of consumer Internet surfing habits by technology companies, advertisers, Internet service providers and Web businesses that focus on consumers on the basis of online behavior. Since 2009 there is a law in Europe that regulates software cookies, but presently there is a move towards allowing the online advertising industry to self-regulate their cookies. However, regulators representing E.U. member states backed by consumers' rights groups have recoiled at the voluntary arrangement, arguing that it does not adequately protect individuals from involuntarily permitting marketers to collect personal data (O'Brien, 2011).

On July 31, 2012, the Commission Nationale de l'Informatique et des Libertés (CNIL), the French privacy protection agency, asked Google to examine private information that cars taking pictures for its Street View service collected, after Google acknowledged that it had retained some of the information despite promising to delete it (Pfanner, 2012). A week earlier, the Information Commissioner's Office of Britain made the same request. Google maintains that it never intended to collect the data, and that it was the result of mistakes by an engineer working on the Street View program. The company had promised to destroy the information but acknowledged it had not actually deleted all of it (Pfanner, 2012).

On August 9, 2012, as we were completing this article, the Federal Trade Commission fined Google $22.5 million to settle charges that it had bypassed privacy settings in Apple's Safari browser to be able to track users of the browser and show them advertisements, in violation of an earlier privacy settlement with the agency (Miller, 2012). Google once again claimed that its actions had been unintentional and were the result of change in Safari of which Google was unaware. Once they were made aware of it, Google claimed that it stopped tracking Safari users and showing them personalized ads. According to Miller (2012), several analysts have questioned the commission's power to effectively police tech companies, which have repeatedly settled privacy violations with the commission. The consensus is that federal regulators do not have enough financing or the legal authority to sufficiently monitor and punish tech companies for privacy violations. Sadly, the same can be said of international counterparts.

CLOSING REMARKS

International trade has undergone a wholesale revolution because of the growth in the use of the Internet by both sellers and buyers. The growing use of search engines to navigate the Internet, the evolution of smartphones that allow individuals access to the Internet wherever they are (via browsers or third-party apps), and the success of social media sites like Facebook.com have afforded us some major opportunities for businesses, but these do not come without major challenges. Social media gives people today the sense of community and closeness. Unfortunately with new social media, an argument can be made that a person's privacy can start to diminish. The Internet is one of the best tools in which marketers

track customer buying behavior patterns for a company. Unfortunately this can sometimes affect people's privacy. According to Lohr (2010a) Congress and the Federal Trade Commission are mulling tighter restrictions on online data collection, disclosure and use. A group of privacy groups sent their principles for controlling data collection and use, in a letter sent to members of Congress on Monday, April 26, 2010. The groups include the Center for Digital Democracy, the Consumer Federation of America, the Electronic Frontier Foundation, the United States Public Interest Research Group and the World Privacy Forum. Their suggested steps include limiting the ability of web sites and ad networks to use behavioral data to 24 hours after it is collected, and requiring consumers' permission — an opt-in approach — to hold such data beyond 24 hours (Lohr 2010a). In addition these privacy advocacy groups say that people should be aware and informed about who is tracking their web browsing patterns and that individuals should have the option to remove their personal data from the tracker's database.

Among all the uncertainties that we face, we know for sure that marketing and international trade are now intricately connected to the Internet. Because of this, the issue of online of privacy will continue to be a concern and source of skepticism for consumers and a challenge to global marketers. For consumers, their apprehension is enhanced by confusion regarding what companies and/or governments may and may not do with the information that they gather from customers via web-based transactions. A related issue is whether private information should be kept online indefinitely. From a government's perspective, as more of our economic activity becomes web-based or web-oriented, a country's economy becomes more susceptible to cyberterrorism attacks that ripple into the global economy. Should regulations need to be set now to protect online privacy or should we allow marketers to self-regulate?

Presently, there are no uniform international laws to deal with violations to online privacy. Thus, we are confronted with the dilemma of having no one specifically monitoring for potential violations to consumers' rights to privacy online. Last, it is becoming critical to ascertain the effectiveness of opt out options and their impact on alleviating consumer skepticism.

REFERENCES

Butterworth, S. & Bowcott, O. (2011), "Privacy online – it's complicated," at http://www.guardian.co.uk/ law/ butterworth-and-bowcott-on-law/2011/apr/15/privacy-online-its-complicated-law.

Choney, S. (2010), "iPad 3G Owners' E-Mail Addresses Hacked," June 9, 2010, at http://www.msnbc. msn.com/id/37602751/ns/technology_and_science-tech_and_gadgets/.

Federal Trade Commission (FTC) (2010), "A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," Bureau of Consumer Protection, December 1, at www.ftc.gov/os/2010/12/ 101201privacyreport.pdf .

Fougner, J. (2010), "Introducing Deals," *The Facebook Blog*, November 3, 2010 at http://blog.facebook.com/blog.php?post=446183422130.

Hester, T. (2008), "*NJ* justices call e-privacy surfers' right," *The Star Ledger,* April 22, 2008, Front Cover.

Helft, M. (2010), "Facebook Vows to Fix a Flaw in Data Privacy," *N.Y. Times*, October 19, 2010 at B8, and http://www.nytimes.com/2010/10/19/technology/19facebook.html?scp=1&sq=facebook%20vows% 2 0to%20fix&st=Search.

Hoofnagle, Chris Jay (2005), "Privacy Self-Regulation: A Decade of Disappointment," Electron-ic Privacy Information Center, at http://www.epic.org/reports/decadedisappoint.pdf.

Hunter, R.J., H.R. Lozada & Mayo, A. (2010), "Censorship in the Video Game Industry: Government Intervention or Parental Controls?" *University of Denver Sports & Entertainment Law Journa*l, Vol. 9 (Fall), 54-72.

Internet World Statistics (2012), *Top 20 Countries with Highest Number of Internet Users*, at http://www.internetworldstats.com/top20.htm.

Internet World Statistics (2012a), *Top 58 Countries with the Highest Internet Penetration Rate*, at http://www.internetworldstats.com/top25.htm.

Kerry, J. (2011), "Kerry, McCain Introduce Commercial Privacy Bi-Partisan Legislation Would Enhance Protection and Control of Personal Information," April 12, at http://kerry.senate.gov/press/release/?id=59a56001-5430-4b6d-b476-460040de027b**.**

Kerry, J. (2011a), "Commercial Privacy Bill of Rights," (summary), April, at http://kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-9709-1cb51c6759e6&CFID= 81774630&CFTOKEN= 59178535.

Lavin, M. (2006), "Cookies: What Do Consumers Know and What Can They Learn?" *Journal of Targeting, Measurement, and Analysis for Marketing*, 14 (July), 279-288.

Lee, E. (2011**),** "Proposed Privacy Law Serves Notice to Online Ad Companies: Bipartisan Bill Means to Codify Current Practices, Centralize Various Efforts," *Advertising Age* (April 12), at http://adage.com/article/digital/sens-john-mccain-john-kerry-intro-online-privacy-bill/226948/.

Lee, E. (2010), "Twitter Begins Publishing Ads in Users' Streams," *Advertising Age* (November 1), at http://adage.com/article/digital/twitter-releases-ads-timelines-starbucks-virgin/146822/.

Lohr, S. (2010), "Privacy Concerns Limit Online Ads," *New York Times* at http://bits.blogs.nytimes.com/2010/04/30/privacy-concerns-limit-online-ads-study-says/.

Lohr, S. (2010a), "How Privacy Vanishes Online," *New York Times* at http://www.nytimes.com/2010/03/17/technology/17privacy.html (last accessed August 12, 2012).

Martin, D., Wu, H., & Alsaid, A. (2003), "Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use," *Communications of the ACM*, 46 (December), 258-264.

Miller, C.C. (2012), "F.T.C. Fines Google $22.5 Million for Safari Privacy Violations," *New York Times*, at http://bits.blogs.nytimes.com/2012/08/09/f-t-c-fines-google-22-5-million-for-safari-privacy-violations/.

Miyazaki, A.D. (2008), "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," *Journal of Public Policy & Marketing*, Vol. 27, (1), 19-33.National Advertising Initiative (2010), "About the NAI," at http://www.networkadvertising.org/about/.

National Advertising Initiative (NAI) (2010), "About the NAI," at http://www.networkadvertising.org/about/.

O'Brien, K.J. (2011), "Setting Boundaries for Internet Privacy," *N.Y. Times*, September 18, 2011, at B8 and http://www.nytimes.com/2011/09/19/technology/internet/setting-boundaries-for-internet-privacy.html?r=1&scp=1&sq=privacy%20and%20internet&st=cse.

Pfanner, E. (2012), "Google Failed to Delete Street View Data in France," *New York Times* at http://www.nytimes.com/2012/08/01/technology/01iht-google01.html?_r=1&ref=technology.

Phelps, J., Nowak, G., & Ferrell, E (2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, Spring: 19 (1), 27-41.

Privacy Rights Clearinghouse (2012), *Online Privacy: Using the Internet Safely*, at https://www.privacyrights.org/ fs/fs18-cyb.htm.

Raghu, T.S., Kannan, P.K., Rao, H.R., & Whinston, A.B. (2001), "Dynamic Profiling of Consumers for Customized Offerings over the Internet: A Model and Analysis," *Decision Support Systems*, 32 (December), 117-134.

Vega, T. (2010), "Code That Tracks Users' Browsing Prompts Lawsuits," *New York Times* at http://www.nytimes.com/2010/09/21/technology/21cookie.html?pagewanted=all.

Vega, T. & Kopytoff, V. (2010), "In Online Privacy Plan, the Opt-Out Question Looms," *New York Times*, December 5, 2010, at http://www.nytimes.com/2010/12/06/business/media/06privacy.html.

U.S. Department of Justice (2010), "Justice Information Sharing: Privacy & Civil Liberties," at http://it.ojp.gov/default.aspx?area=privacy&page=1285.

The authors want to thank the Institute for International Business in the Stillman School of Business at Seton Hall University for its support of this research.