Wrestling With Consumer Privacy on the Internet

With estimates placing the value of commerce transacted over the Internet by consumers in the hundreds of billions of dollars, it is not surprising that consumer privacy on the Internet is a hot issue these days. This fact has not been lost on the Federal Trade Commission, which is in the middle of hosting a series of day-long roundtable discussions entitled "Exploring Privacy." The second in the roundtable workshops will be held at Berkeley School of Law later this month on January 28.

SEAN MORRIS, a partner in Arnold & Porter's Los Angeles office, specializes in complex commercial litigation with particular emphasis on intellectual property and technology issues.

The Internet provides businesses with unique opportunities to learn facts about consumers so that they then can better interact with and serve customers. For example, businesses that know what a customer likes (based on what is purchased or browsed) can tailor communications to topics that the customer might find useful. At the same time, consumers want to understand what information about them is being collected and how it is being used or stored, as well as to have the ability to restrict transmission of particularly sensitive information. Recent reported changes to privacy setting options and policies announced by popular companies such as Google and Facebook highlight the importance of this issue both for businesses and consumers.

SUZANNE WILSON is a partner in Arnold & Porter's Los Angeles office. She represents Internet and technology companies, as well as consumer product companies and other businesses in commercial and intellectual property litigation.

The FTC has been wrestling with Internet privacy issues for well over a decade, but recent years have seen an increased focus on the topic. In 2006, the FTC hosted hearings over a four-day period on "Protecting Consumers in the Next Tech-ade." Those hearings, which brought together a mix of speakers and technology experts, covered a wide-range of e-commerce issues, with consumer privacy playing a prominent role. Indeed, a stated goal of the "Tech-ade" hearings was to create an opportunity for the FTC to learn more about technological changes in the marketplace so that it could assess their effects on consumer privacy. And, in the report that followed the conference, the FTC listed one of its future "primary objectives" as "[e]nsuring that consumers' private information, which will increasingly be collected, stored, and used in both marketing and payment, is maintained securely."

In pursing this "primary objective," over the last year or so the FTC issued several "guidelines" or "best practices" designed to guide businesses regarding e-commerce privacy. These publications included items such as the "Self-Regulatory Principles For Online Behavioral Advertising," which was intended to serve as a tool for businesses to self-regulate the manner in which they used consumer data to track online activities and to deliver targeted advertising.

In addition to issuing such guidelines, the FTC also recently has been active using its existing enforcement powers to try to address privacy issues. For example, in 2009, the FTC filed a complaint against a major retailer regarding its use of a computer program to collect customer data. The retailer had solicited volunteers from among its customers to agree to place a program on their computers that would monitor Internet browsing. The data collected by the computer program then would be used by the retailer as research to obtain a better understanding of consumers' needs. Although the retailer disclosed to the volunteers how the program would work (and included a $10 payment for people who volunteered) and the customers affirmatively opted in to participate, the FTC asserted in its complaint that the form of disclosure was not sufficient and was in violation of Section 5 of the Federal Trade Commission Act (which broadly governs actions the FTC perceives to be unfair or deceptive).

The FTC and retailer eventually settled the case by entering into an agreement not to further disseminate any similar computer tracking program without a more detailed disclosure about the program being provided on a "separate screen" apart from any general end-user license agreements or other "terms of use." This and other cases reflect that the FTC, even as it was issuing self-regulatory principles, was prepared to act under its current enforcement powers to take on privacy issues where it saw them.

The FTC is not the only government entity working through these issues; Congress also has been active. Following a series of hearings of its own over the last couple of years, Congress is showing interest in developing a general national consumer privacy bill. For example, Congressman Rick Boucher (D-Va), who is the head of the Communications, Technology and the Internet subcommittee of the House Energy and Commerce Committee, is reportedly overseeing draft legislation that would address Internet commerce issues such as data collection limits, increased consumer notice and transparency, and enforcement.

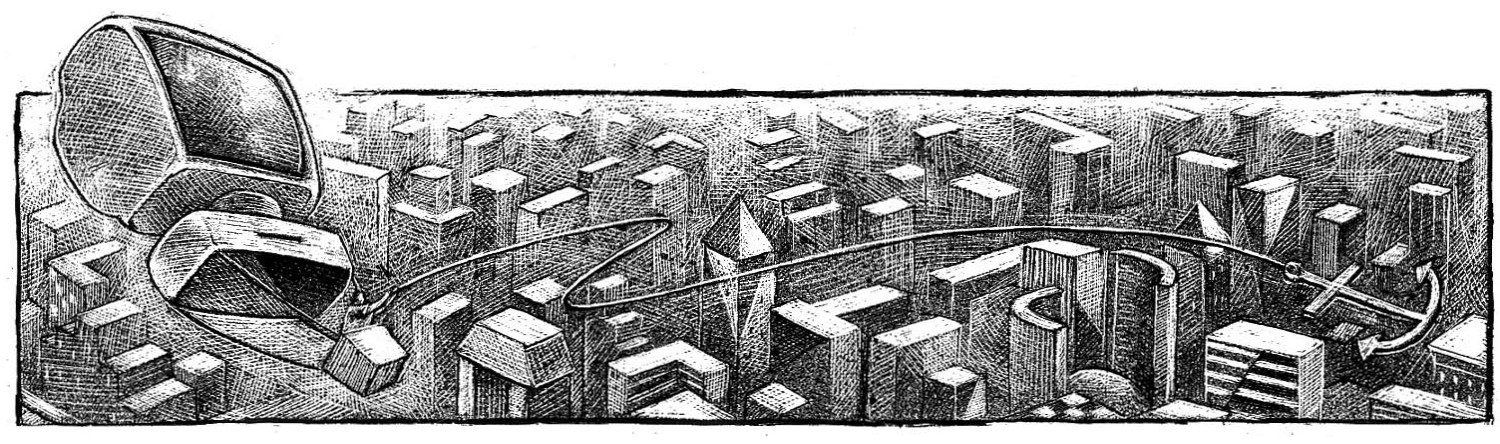
Against this backdrop, the FTC has begun hosting its privacy roundtable discussions in an effort to explore further how e-commerce can continue to be conducted efficiently while at the same time protecting consumers. Billed as forums to "explore the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data," the FTC has stated that it is interested in considering "how best to protect consumer privacy while supporting beneficial uses of the information and technological innovation."

The FTC has begun hosting privacy roundtable discussions in an effort to explore further how e-commerce can continue to be conducted efficiently while at the same time protecting consumers.

To generate robust discussion on these topics, the FTC invited a wide-array of panelists (representing business, consumer groups, technology, and government) to present their views at the first roundtable held last month. FTC Chairman Jon Leibowitz opened the discussions by referring to this as a "watershed moment in privacy." The panelists then debated, sometimes heatedly, the benefits and risks of collection and use of consumer data over the Internet.

For the second roundtable later this month, the FTC again has invited distinguished panelists representing different points-of-view to discuss these issues. The FTC asked contributors to focus on two particular questions: What role do privacy enhancing technologies play in addressing Internet-related privacy concerns? What challenges do innovations in the digital environment pose for consumer privacy? How can those challenges be addressed without stifling innovation or otherwise undermining benefits to consumers?

It will be interesting to hear the panelists discuss these topics, and even more interesting to hear reactions from the FTC. As it has recognized, the FTC must walk a line between efforts to protect consumers in their e-commerce activities and not interfering with beneficial business practices that actually enhance users' online experiences. As David Vladeck, the FTC Director for the Bureau of Consumer Protection, noted when summing up the last discussion, the debate among the first roundtable panelists exemplified "just how difficult the questions we have to confront are." The second roundtable undoubtedly will confirm this sentiment.



E-Discovery Reflections of 2009

This year the case law at both a state and federal level matured, with the end game still being that reasonableness, common sense and good faith are the underlying tenants guiding document discovery.

The federal courts emphasized that document requests balance the cost-reward ratio and rest on some demonstrative basis for the request beyond gut instinct. *See e.g., Ford Motor Co. v. Edgewood Props., Inc.*, 257 F.R.D. 418 (D.N.J. 2009) (should requesting parties fail to make a demonstrative showing that opposing counsel acted in either a purposeful or negligent manner in withholding documents, the court will deny the requesting party demand - weighing the reasonableness of the demand against the cost.); *William A. Gross. Constr. Assocs., Inc. v. Am. Mfrs. Mut. Ins. Co.*, 2009 WL 724954 (S.D.N.Y. Mar. 19, 2009); *Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dept. of Homeland Sec.*, 2008 WL 5062700 (S.D.N.Y. Nov. 21, 2008).

DANIEL B. GARRIE, Esq. has a B.A. and M.A. in computer science and is an e-discovery neutral and special master with ARC. He is on the Board of Advisors to Digital Reef Inc. and was named 2009 Top Neutrals as an Up and Coming Neutral. He can be reached at (310) 284-8224 and DGarrie@fsrdg.com.

Common sense rules are also in state courts. For instance, when a litigant directly violates a court order to produce their laptop by using wiping software to delete potentially relevant data, sanctions will be issued. *See Oz Optics, Ltd. v. Hakimoglu*, 2009 WL 1017042 (Cal. App. Apr. 15, 2009) (Unpublished). Counsel in receipt of a litigation hold, or certainly a court order, should advise their client to comply and provide guidance on compliance where necessary to avoid negative results and sanctions. *See e.g., Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 4858685 (S.D. Cal. Nov. 7, 2008); *Keithley v. Home Store.com, Inc.*, 2008 WL 3833384 (N.D. Cal. Aug. 12, 2008); *R & R Sails Inc. v. Ins. Co. of Pa.*, 251 F.R.D. 520 (S.D. Cal. 2008); *In re Flash Memory Antitrust Litig.*, 2008 WL 1831668 (N.D. Cal. Apr. 22, 2008)(discussing importance of counsel's role in execution of preservation dollars).

This is not to say that the massive amount of information created and stored by an organization does not present an operational challenge to the legal and technology and potential e-discovery risks when a response to a discovery request comes via the courts or administrative agency. In 2009, the case law and stories reported demonstrated that a great deal of e-discovery headaches arise from the copious amounts of unstructured and unmanaged electronically stored information.

Arguably, legal fees have not grown a great deal in proportion to the amount of data being requested, reviewed and produced. Clients should realize that greater cost savings can be achieved by focusing on addressing the issues of controlling the amount of information existing within an organization. While anecdotal, the case law and conversations with my peers, suggest that a clients inability to control their data escalates the costs of e-discovery and not the legal fees. Effectively less information results in a proportional reduction in the amount of information that is reviewed for legal matters when examined over an extended period - information being defined uniquely for each company and assuming that the systems captures all relevant content.

Counsel should seek solutions that transform an e-discovery request from an unwelcome pressure point to a demonstration of the organization's capability to marshal its enterprise content with minimal disruption to ongoing business operations.

The coming year will certainly be a big one for e-discovery as the Supreme Court will hear the 9th Circuit's decision in *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008). It is foreseeable that the Supreme Court may elect to use this case to shape privacy rights of U.S. citizens and weight in on the scope of e-discovery.

Below are a couple of good axioms lawyers, for big or small companies or firms, might want to apply in 2010 when dealing with e-discovery.

"Trust but verify." It is important that counsel inquire whether cases cited to by vendors in a white paper or presentation have been shepardized, requesting a copy of the case where appropriate. Vendors can unknowingly cite to case law that is no good, or broadly reference and apply cases limited to a unique set of facts. Trust and verify equally applies to counsel's dealing with in-house information system managers and information custodians - it is rare that the first answer is the complete answer.

"Use it or lose it," meaning "Does a vendor eat their own dog food." This asks whether the vendor uses its own product. If the vendor does not, this should raise a red flag.

It was a watershed year for e-discovery and 2010 is likely to be even more telling.