FTC Hosts Workshop on Comprehensive Consumer Data Collection

Dana B. Rosenfeld, Alysa Z. Hutnik

December 11, 2012

On December 6, 2012, the Federal Trade Commission ("FTC") hosted the public workshop, "The Big Picture – Comprehensive Online Data Collection," which focused on the privacy concerns relating to the comprehensive collection of consumer online data by Internet service providers ("ISPs"), operating systems, browsers, search engines, and social media. The workshop, which fulfilled an action item contained in the FTC's March 2012 final privacy report, featured a series of panels with representatives from government, academia, consumer groups, privacy professionals, and the technology industry who discussed the risks and benefits, consumer awareness and perceptions, and the future of online data collection.

According to the Commission, the purpose of the workshop was to identify differences in how existing online technologies collect consumer data, and determine whether these differences should have any bearing on current privacy policy discussions. The FTC and other stakeholders will use the information obtained during the workshop to assess whether certain technologies, such as deep packet inspection ("DPI"), warrant heightened restrictions or enhanced consumer consent requirements.

"Databases of Ruin"

FTC Commissioner Julie Brill introduced the first panel by describing the extent to which service providers can now collect data about computer users across unaffiliated websites, including when some entities have no direct relationship with such users. She also noted that ISPs, which serve as an Internet gateway for their customers, have access to large amounts of unencrypted data that their customers send and receive. Using technologies such as DPI, this information potentially could be used to develop highly detailed and comprehensive customer profiles through a process that is invisible to customers. According to Commissioner Brill, in the absence of effective privacy controls or regulations, these profiles could amount to "databases of ruin," a phrase coined by the FTC Senior Advisor Paul Ohm to describe aggregated data sources that can negatively impact a person's reputation, employment prospects, and relationships.

As a follow-up to Commissioner Brill's remarks, Professor Dan Wallach from Rice University provided an overview of the technological landscape of comprehensive data collection, including the methods by which data collection occurs, and how a combination of first-party collection (such as a supermarket rewards card) and third-party collection (such as when a consumer's data or transaction history is sold to a third-party) can lead to powerful inferences about a consumer's behavior and likely purchases, as well as that consumer's friends' and neighbors' behavior.

Benefits and Risks of Comprehensive Data Collection

The first panel explored both the consumer benefits and the privacy concerns associated with technologies that have the ability to track all, or virtually all, of a consumer's online activities. Mike Altschul, Senior Vice President and General Counsel at CTIA — The Wireless Association, argued that comprehensive data collection and aggregation are "making information visible," which, in turn, allows public and private entities to provide novel public benefits such as identifying contagious disease outbreaks, improving traffic patterns through geolocational data, and developing new products and services that are specifically targeted to consumer preferences. Similarly, Howard Beales, former FTC Director of the Bureau of Consumer Protection and current professor at George Washington University, asserted that comprehensive data collection remains the driver of the advertiser-supported business model that enables the free online content and services that consumers have come to expect.

Professor Beales further stated that there is no single technology or chokepoint that necessitates additional regulation because a consumer's online conduct remains highly fragmented (that is, the consumer likely has multiple devices that use multiple networks provided by multiple service providers), which inhibits the ability of a single entity to build a comprehensive profile on an individual. According to Professor Beales, "[i]f you can't articulate what the harm is, then you can't prevent it" and any action focusing only on speculative harm will restrict future industry advancements. Markham Erickson, General Counsel at the Internet Association, agreed with Professor Beales and cautioned that policymakers must first clearly identify the harms they are seeking to prevent and must avoid imposing rules that simply focus on data collection.

In contrast, Professor Neil Richards, from the Washington University in St. Louis School of Law, described how comprehensive data collection infringes on the concept of "intellectual privacy," which is predicated on consumers' ability to freely search, interact, and express themselves online. Professor Richards also stated that comprehensive data collection is creating a transformational power shift in which businesses can effectively persuade consumers based on their knowledge of consumer preferences, yet few consumers actually understand "the basis of the bargain," or the extent to which their information is being collected. Independent technology consultant Ashkan Soltani offered that online information is "co-owned" by the people who generate the data and the entities that offer services to access such data. Thus, according to Mr. Soltani, businesses must be mindful when collecting data for one purpose and then using it for another unknown purpose.

Mr. Soltani also disputed Professor Beales' comments on the extent of data fragmentation and noted that more consumers now access the same online application from different devices, which gives the app powerful data on consumers' use preferences. Similarly, Lee Tien, a senior staff attorney with the Electronic Frontier Foundation, described a "fairness problem," in which consumers are being induced into providing information about themselves with no understanding about who is collecting the information and how it is being used. He noted that, once disparate information about a consumer is collected and stored, it has a tendency to aggregate together in the absence of regulation or technical siloing.

On the specific topic of DPI technology, Mr. Altschul asserted that DPI has been unnecessarily demonized, and that regulators should not focus on any specific technology. Similarly, Mr. Erickson commented that it is not effective to base policy decisions on a specific technology such as DPI given how quickly technology changes. Professor Richards compared DPI to a gun, a car, or a kitchen knife; that is, whether it is good or bad depends upon how businesses decide to use it. In contrast, Mr. Tien said that, regardless of how the data is used, DPI is no different than the phone company

listening into phone calls without the caller's knowledge or consent.

"Avoid Picking Winners and Losers"

As a lead in to the second workshop panel, FTC Commissioner Maureen Ohlhausen discussed the need for balance between imposing new privacy controls and continuing to encourage online innovation. She echoed the earlier comments by Mr. Altschul and Professor Beales that policymakers should focus on the harm to consumers rather than "picking winners and losers" based on a particular technology. Thus, she advocated for providing consumers with more tools that include a mix of marketplace-based approaches and self-regulation.

Consumer Attitudes About Choice with Respect to Comprehensive Data Collection

The second panel focused on consumer knowledge and attitudes regarding comprehensive data collection, the role of consumer choice and transparency, and how to make consumer choice meaningful. Michael Hintze, Associate General Counsel at Microsoft, opened the discussion by stating that there is a large gap between what companies could collect and what they actually do collect. He argued that most companies deliberately limit the data they collect in response to consumer privacy concerns, and they apply a common sense approach that is not designed to trick consumers. According to Mr. Hintze, if an entity wishes to change the terms after it obtains initial consumer consent, it must provide clear notice.

In contrast, Lorrie Faith Cranor, a professor at Carnegie Mellon University, cited recent studies showing that a large number of consumers are confused and have little to no understanding about online data tracking. Thus, notice by itself is not the answer. Rather, the timing and format of the notice must be carefully considered and the notice must be accompanied by meaningful choice. The present challenge, according to Professor Cranor, is that data collection is happening continuously and consumers will ignore a constant barrage of privacy notices. She also stated that, while the notice and transparency recommendations in the FTC privacy framework provide useful guidance, they are too vague to provide industry with a truly meaningful roadmap.

Christopher Calabrese, Legislative Counsel with the American Civil Liberties Union, agreed with Professor Cranor and argued that the current frameworks are insufficient to protect consumers. In his view, legislation, not self-regulation, is needed to make consumer privacy rights meaningful and fully understandable to consumers. Further, in response to statements in the first panel, Mr. Calabrese argued that basing any new regulations on harm alone is an ineffective approach because, in many cases, consumers may not even realize they have been harmed (such as in the case where a consumer is unaware that he or she was given a higher insurance rate).

The Future of Comprehensive Data Collection

The third and final panel focused on possible next steps for industry and policy makers in the area of comprehensive data collection, including the standards that should apply to certain types of data collection, and whether the market can provide alternatives for consumers who wish to avoid having their data collected.

Thomas Lenard, President and Senior Fellow at the Technology Policy Institute, echoed panelists' earlier comments that there must be evidence of systematic harm before the government imposes new regulations, and he warned against regulating to address hypothetical harms that have yet to occur. According to Mr. Lenard, consumers largely understand the "rough bargain" they make when

they use free online services, and that most consumers are not truly interested in the details of how online data collection occurs.

In contrast, Chris Jay Hoofnagle, Director of Information Privacy Programs at the Berkeley Center for Law & Technology at the Berkeley School of Law, described comprehensive data collection as "surveillance" that causes harm simply because it infringes upon every consumers' "space to play" and free expression, regardless of any quantifiable economic harm. Further, in response to Mr. Lenard's comments that most consumers are not interested in the specifics of online data collection, Mr. Hoofnagle stated that when consumers are given clear information and a convenient way to exercise meaningful choice — such as with the National Do Not Call Registry to prevent unwanted telemarketing calls — consumers will rush to it.

Randal C. Picker, a professor at the University of Chicago School of Law, cautioned that consumers also need to realize that "privacy by design" comes with a cost because it can limit innovation, and that government must tread lightly to ensure that it does not unduly restrain the next generation of innovators through over-regulation. As a final thought for the panel, Sid Stamm, Lead Privacy Engineer at Mozilla, advocated for sensible settings and described the industry's continuing search for "the holy grail," which includes a balance that involves giving developers an incentive to continue improving the user experience, yet ensuring that (1) consumers are aware of the information collected about them and (2) that this information remains safe once collected.

Conclusion

The topic and timing of the workshop provide clear indicators that consumer online privacy will remain an important area of focus for the Commission in 2013, both in terms of enforcement and potential policy initiatives. The workshop also served as a reminder that, in the absence of federal consumer privacy legislation and to avoid regulator scrutiny in the year ahead, online businesses that collect customer information should continue to apply the three core recommendations stated in the FTC's March 2012 privacy framework: "privacy by design," providing simplified privacy choices to consumers, and providing greater transparency about data collection and use.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

For more information about this advisory, contact:

Dana Rosenfeld
(202) 342-8588
drosenfeld@kelleydrye.com

Alysa Hutnik
(202) 342-8603

ahutnik@kelleydrye.com