wiley

NEWSLETTER

FTC PrivacyCon 2018 Examines Opportunities and Challenges in Privacy and Data Security

March 2018

Privacy in Focus®

On February 28, 2018, the Federal Trade Commission (FTC or Commission) hosted PrivacyCon 2018. The conference featured the presentation and discussion of original research completed during the prior two years. It explored a variety of privacy and cybersecurity issues in the Internet ecosystem. The FTC's stated objective was to examine the privacy and security implications of emerging technologies. Companies should expect the FTC to remain vigilant about new products and services, and the conference previewed a number of potential action areas.

The Conference

Acting FTC Chairman Maureen K. Ohlhausen opened the conference by highlighting recent FTC privacy actions and related initiatives. The remainder of the conference was divided into four sessions, each focusing on a distinct area of privacy and data protection. The panelists brought a variety of expertise in topics that ranged from the exfiltration of personal data by session-replay scripts to consumer expectations regarding Internet-connected toys.

Session 1: Collection, Exfiltration, and Leakage of Private Information

- Steven Englehardt, Ph.D. candidate at Princeton University, discussed email tracking. He claimed that many of the top web trackers are now in emails, and the line between email and web tracking has been blurred.
- Michael Weissbacher, doctoral student at Northeastern University, focused on browser extensions. According to Weissbacher, these extensions often leak complete consumer browsing history to third parties.
- Milijana Surbatovich, Ph.D. candidate at Carnegie Mellon University (CMU), discussed the use of "if this, then that" applets in the Internet of Things (IoT). She noted research finding that half of all tested applets violated secrecy or data integrity standards.
- Gunes Acar, Postdoctoral Research Associate at Princeton University, focused on session-relay scripts, which record individual browsing sessions (e.g., user scrolls and clicks). Companies often use these

scripts to improve websites, but the recorded sessions can expose passwords, credit and health data, and purchase details.

- Alan Mislove, Associate Professor and Associate Dean at Northeastern University, argued that social networks are modern data brokers and can be misused to link multiple pieces of personally identifiable information (PII) to single users, infer phone numbers, and de-anonymize visitors.

Takeaways: The panelists agreed that unintentionally collecting certain data creates liability risks. They also suggested that the FTC should take steps to encourage transparency on data collection and sharing. To mitigate these risks, companies should continue to find innovative ways to minimize data collection and follow FTC transparency guidelines.

Session 2: Consumer Preferences, Expectations, and Behaviors

- Jingjing Ren, Ph.D. candidate at Northeastern University, discussed data leaks in mobile apps. She emphasized that mobile adoption of https has been slow and that third-party tracking is pervasive and broad.
- Kristopher Micinski, Visiting Professor at Haverford College, discussed permissions on mobile operating systems. He has led two studies examining how apps use permissions and device functionality. The studies found that apps use the most sensitive functions (e.g., cameras and microphones) only when interacting with consumers, while other functions are used more often and without consumer interaction.
- Emily McReynolds, Senior Privacy Manager at Microsoft and former researcher at the University of Washington Tech Policy Lab, highlighted consumer expectations for connected toys. In her research, some parents claimed to not have time to review all required disclosures, while others were concerned about their children's information. When told that they were recorded, the children said it sounded "scary."
- Pardis Emami-Naeini, Ph.D. student at Carnegie Mellon University, discussed expectations and preferences in an IoT world, as well as a mobile application that provides information on nearby IoT devices. She described a survey showing that consumers want to be notified when their data is shared or biometric data is collected. The type of data and perceived benefits mattered most to consumers.
- Yang Wang, Assistant Professor at Syracuse University, explored privacy violations in crowd work (i.e., when a company obtains contributions from an undefined pool of people). He argued that information collection, processing, dissemination, invasion, and deceptive practices are ripe areas of consumer concern.

Takeaways: Consumer expectations are complex and evolving. The FTC noted that it often gets complaints that people do not read privacy policies, and the panelists agreed that the Commission needs to properly scope disclosure requirements to avoid notice fatigue. Companies should consider information sensitivity in tandem with consumer benefits and avoid excessive notifications.

Session 3: Economics, Markets, and Experiments

- Ying Lei Toh, Ph.D. candidate at the Toulouse School of Economics, explored incentives for firms to protect consumer data. Her research focuses on whether data breaches cause reputational damage and found that the answer depends on whether a consumer is both willing and able to punish the firm (e.g., do they know of the breach?). She also noted that mandatory breach notification could hurt investment levels.
- Sasha Romanosky, Policy Researcher at the RAND Corporation, discussed cyber insurance policies and how a lack of data limits insurers' ability to price cyber risks.
- Jaspreet Bhatia, Ph.D. candidate at Carnegie Mellon University, examined empirical measurements of perceived privacy risks, finding that consumers are more likely to share data with government about who they are (e.g., device information, IP address) than what they do online.
- Caleb Fuller, Assistant Professor at Grove City College, considered whether there is a market failure in digital privacy. His research suggests that users are aware of collection practices generally but unaware of specific practices. He claimed that consumers want more privacy, but only 15% are willing to pay for it.
- Christian Catalini, Professor at the Massachusetts Institute of Technology, discussed the digital privacy paradox, in which consumers claim to value privacy but are willing to provide extensive personal data for free services.

Takeaways: Consumers are generally aware of collection policies and believe that information sharing is beneficial. Companies should continue to offer services that consumers value in exchange for the data they collect and share.

Session 4: Tools and Ratings for Privacy Management

- Periwinkle Doerfler, Ph.D. candidate at New York University, discussed the use of mobile spyware in abusive relationships. She demonstrated a mobile app that does not display an icon and records video and audio while the phone appears off.
- Saksham Chitkara, Graduate Research Associate at Carnegie Mellon University, examined context-aware privacy management on smartphones. He claimed that the current app permission structure is a "black box" and that third-party libraries often collect data for which they have no use. He has developed a mobile app, ProtectMyPrivacy, that minimizes data flowing to third-party libraries.
- Ian Douglas, from the Office of the Privacy Commissioner of Canada, discussed IoT privacy in health and medical devices. His research found that the amount of data collected varies; sharing is not as frequent as expected; well-established medical companies have better safeguards; and scrubbing data is not always easy or possible.
- Katie McInnis, Policy Counsel for the Consumers Union, presented privacy and security research on connected televisions.

- Norman Sadeh, Professor at Carnegie Mellon University, discussed "assisting users in a world full of cameras." He found that there are over 6,000 cameras in Times Square alone, with uses that include facial recognition, security, and marketing. He also found that the use of facial recognition is on the rise. He noted that most users claim to want notice and choice for facial recognition, and would disable the feature if given the option.

Takeaways: Data collection and integrity processes vary. Companies should ensure that their processes are properly suited to their use cases.

Conclusion

As the FTC continues to emphasize consumer privacy and data security, companies should be mindful of the issues explored at the conference. Companies should be careful to minimize the data they collect and share; follow FTC transparency guidelines; weigh the sensitivity of consumer information with perceived consumer benefits; offer relevant services that consumers value in exchange for collected data; and ensure that collection and security processes are properly scoped. The U.S. Court of Appeals for the Ninth Circuit recently upheld FTC authority to regulate non-telephone activities of mobile operators and other common carriers, and companies should prepare for increased FTC action in the privacy and security space more generally.