UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Social Media CyberWatch: April 2013

A monthly report on trends in privacy, security,

and governance issues as they relate to social media

Table of Contents

LEGISLATIVE LANDSCAPE

CISPA dead again

This month, the controversial cybersecurity information sharing bill CISPA passed the United States House of Representatives, but was shelved by the Senate, in a repeat of 2011's events when CISPA was initially deliberated. This came after numerous social media campaigns by advocacy groups, lobbying by industry, and a veto threat by the Obama administration. The bill sought to make it easier for private organizations to share information with the United States government about suspected "cyber threats". Perceived problems with the bill included the prioritization of military control of cyber threat information over more transparent civilian agencies, immunity from any damages that arise out of "hacking back" against perceived threats, and thecircumvention of existing privacy protections when providing personal information related to broadly-defined cyber threats to the government.

U.S. warrantless surveillance program highlighted

Celebrations by advocacy groups after the demise of CISPA may have been bittersweet as documents recently obtained by the Electronic Privacy Information Center reveal that even without a law such as

CISPA, the U.S. Justice department has been granting legal immunity to ISPs taking part in a cybersecurity pilot program to intercept communications on portions of their networks without court authorization. This practice would have been formalized by CISPA if it became law. An executive order by President Obama requires Homeland Security to expand this data sharing program to all critical infrastructure sectors.

IRS warrantless email snooping

Documents obtained by the American Civil Liberties Union (ACLU) suggest that the criminal investigative unit within the IRS has obtained emails from service providers without a warrant, contrary to the 2010 Warshak court ruling that decided email can be protected under the U.S. constitution from unreasonable search and seizure. Following the ruling, the ACLU documents suggest that the IRS has continued to obtain such emails. The IRS responded shortly thereafter, denying that it uses emails to "target taxpayers". After pressure from the U.S. Senate to clarify its practices, IRS Acting Commissioner Steven Miller stated that to his knowledge, the IRS has not obtained electronic communications without a warrant, which contradicts information in the obtained documents. Miller further stated the IRS will clarify its policies in the future.

ECPA Amendment to restrict warrantless access to emails proposed

A new U.S. Senate bill to amend the Electronic Communications Privacy Act (ECPA) would require law enforcement to obtain a warrant before compelling service providers to release the contents of users' electronic communications. ECPA currently permits warrantless access to previously-opened emails and those over 180 days in age, practices that would no longer be allowedexcept in emergency situations under the amended Act. Advocacy groups have been calling for modernizing reforms to the 1986 Act for several years.

FBI pursuing real-time social media surveillance powers

A new U.S. Senate bill to amend the Electronic Communications Privacy Act (ECPA) would require law enforcement to obtain a warrant before compelling service providers to release the contents of users' electronic communications. ECPA currently permits warrantless access to previously-opened emails and those over 180 days in age, practices that would no longer be allowedexcept in emergency situations under the amended Act. Advocacy groups have been calling for modernizing reforms to the 1986 Act for several years.

UK criticizes proposed EU "right to be forgotten" regulation

British officials have claimed proposed updates to the EU Data Protection Regulation that would create a so-called "right to be forgotten" will create unrealistic expectations about the reach of the policy. In practice, the proposed legislation would mandate online service providers to take reasonable steps to

erase digital information pertaining to a user at that user's request. Critics point out that such a right would not be as absolute as the title suggests, as the policy would need to be balanced with freedom of expression, scientific research, and other concerns. The UK Ministry of Justice also stated concerns about clauses in the proposal that would require data operators such as online service providers to take steps to manage third parties to delete data as needed, claiming it to be another of the scheme's practical difficulties.

TRACKING REPORTS, FEATURES AND COLLECTIVE ACTION

Reddit users dig up personal information of wrongfully accused

Social media website reddit.com met a significant amount of criticism for the "witch hunt" carried out by some of its users in response Boston marathon bombing. Reddit users collectively analyzed many photographs of the scene and "doxxed" individuals thought to be suspicious, unearthing social media profiles and other personal information. The New York Post later published those individuals' photos on its front page, alleging they were suspects in the case. After the FBI came forward and dismissed the credibility of the photos, administrators of the site apologized for the incidents and noted that while it has a policy barring the publication of personal information, the policy had been ineffective. The events highlight that crowdsourced activities do not necessarily produce ideal results, though there are many examples of crowdsourced action helping manage crisis situations.

Google releases latest Transparency Report

Google's Transparency Report for the latter half of 2012 indicates a continuation of the trend for increased requests to user data, and increased requests for content removal from governments. The report highlights the fact that 17 governments requested Google remove the controversial video "Innocence of Muslims". A Google public policy blog post notes that this period saw a large increase in content removal requests from the Brazilian government, most of it pertaining to municipal elections and alleged defamation of political candidates. The report also reveals that total government requests for user data and content removalscontinue to increase, while Google's compliance rate to such requests has been gradually declining, but remains slightly below 50 percent overall.

Facebook emoticons add structured data to posts

A new feature on the Facebook platform encourages users to select from a drop down of "emoticons" that suggest what you might be feeling, watching or eating at the moment. A blog post on Slate suggests that this feature is meant to enlist users in adding structured data points to the generally unstructured data of status updates, after natural language processing proved too challenging to execute reliably. The blog posits that this structured data will help Facebook to develop a more accurate profile of users and serve them more tailored ads.

Data brokers + Facebook

The Electronic Frontier Foundation recently published an in-depth look into how Facebook interacts with data brokers to serve targeted ads to its users. The report outlines how Facebook can target ads based on broker data without directly exchanging personal information, best practices for opting out of data broker programs and protecting yourself from third-party data collection. This comes as Facebook continues to describe its relationship with data brokers, which sees it leveraging information about its user's offline behaviours and interests in order to build its partner categories service that enables advertisers to more efficiently target interest groups on the social network.

Read previous editions of the Social Media CyberWatch.