TECHNOLOGY

Naked in a steam room: The new face of privacy

Hacker convention features latest tools for consumer counter surveillance

July 21, 2014 10:00AM ET

by **Chris Francescani** - @CDFrancescani


Hope X

The Hope X conference in New York, July 19, 2014. Chris Francescani

NEW YORK — Dark Mail. Blackphones. Secure e-drops. Bitcoin ATMs. Makeup that thwarts facial recognition software. Lock-picking and elevator-hacking tutorials. Disruptive ad blockers.

The latest tools for consumer countersurveillance and evasion technology were on display last weekend as thousands of tech experts, civil libertarians and whistleblowers gathered at the 10th Hackers on Planet Earth (Hope X) conference in Manhattan to reassess emerging threats to privacy and confidentiality in the digital and physical worlds.

The consensus among attendees was clear: Privacy is dead.

“You’d have to be naked in a steam room on top of a mountain if you want to have a truly confidential conversation,” said conference speaker Steve Rambam, a private investigator. “And it has to be your steam room.”

Coding privacy into software

More than a year into former National Security Agency contractor Edward Snowden’s ongoing surveillance revelations, Hope X speakers urged the global hacker community to look beyond NSA programs and how to perfect email encryption to broader concerns about physical surveillance and corporate as well as government data collection.

Snowden, who spoke to attendees via satellite on Saturday, made an impassioned plea to coders and software designers to create new countersurveillance tools and secure communications software.

He challenged them to “build a better future by encoding our rights into the programs and protocols upon which we rely every day.”

Snowden said mass federal data collection is aimed less at reading your emails than keeping a record of your associations. Federal intelligence agencies, he said, want most to know things that a private investigator who personally shadowed you would learn — “who you meet, who you talk to, when it happens, where it was at, not the exact contents of what was said.”

“So encryption protects content, but we forget about associations, and that’s what these programs are all about.”

“It’s not about surveilling you,” he said later. “It’s not about surveilling me. It’s about surveilling us, collectively."

An interchangeable threat

Conference experts said that the broader and growing threats to privacy and confidentiality come from corporations and private defense contractors.

“Ten years ago, there were private-sector attacks on your privacy, and there were public-sector attacks on your privacy. Today they’re interchangeable,” said Rambam, in a custom-made Italian suit and tie, who then wandered off toward the lectern through a sea of black T-shirts and neon-colored hairstyles. He was famously arrested by the FBI at the 2006 Hope conference — on charges of interfering with a federal money-laundering prosecution — making him a legend among hackers.

Rambam, who was cleared of the charges but retains a healthy resentment of federal law enforcement, said that in recent years data collection by government agencies has been far outpaced by that by corporations, including Vigilant Solutions, which owns a 2.5 billion license plate database — the world’s largest and reportedly growing by 70 million new scans a month — that serves more than 2,000 intelligence and law enforcement agencies, from the U.S. Department of Homeland Security down to local law enforcement.

With private-sector data collection, “there’s no need for a warrant,” said Rambam. “It’s a private business record. There’s no [Freedom of Information Act] for Microsoft. And they can do whatever they want with it.”

Dark Mail and ad blockers

Hope X

A bitcoin ATM at Hope X. Chris Francescani

Among the most popular gadgets and software featured at the 10th biennial Hope conference were Dark Mail, a new end-to-end encrypted email service being developed by Lavabit founder Ladar Levison and Silent Circle, makers of the new Blackphone, an Android smartphone configured for privacy and retailing for $679; SecureDrop, a WikiLeaks-like product designed by the Freedom of the Press Foundation to help whistleblowers leak documents to journalists; an alternative currency bitcoin ATM; and “disruptive wearable technology,” a coat that prevents your cellphone from emitting Wi-Fi signals; hair extensions and make up that camouflage your face from facial recognition cameras; and an umbrella lined with tiny infrared sensors invisible to the human eye that blind surveillance cameras and prevent identification.

Some new software featured at Hope X is aimed at utility as well as consumer dissent.

Daniel Howe, a researcher with a Ph.D in computer science, said he is getting ready to launch AdNauseam, a disruptive ad blocker browser extension that dilutes your data profile collected by ad-tracking software.

The plug-in works like most ad blockers — preventing pop-up ads — but behind the scenes, the AdNauseam clicks on every single advertisement on a page, creating what data miners call noise — inaccurate or unusable information.

“AdNauseam introduces antagonism between the advertisers and the ad network,” said Howe. His 2012 TrackMeNot browser extension was the first to be put into widespread use to prevent advertiser cookies from following a user from website to website.

Howe said he was roundly criticized by data collectors and the security industry after TrackMeNot and debated Google’s general counsel at a forum at New York University. He said he has been the target of ethical criticisms of his software projects.

Critics have told him he was “wasting bandwidth and storage space and if everyone did this at the same time, the Internet would come crashing down,” he said over lunch on Friday. “But why is it wasteful to use this little bit of bandwidth to try and protect my privacy and register my dissatisfaction with the state of the industry? Couldn’t you just as easily argue that it’s a waste of bandwidth and storage space to download that 10 gigs of porn?”

Digital data “obfuscation is a temporary, specific strategy, a short-term solution during a time when it’s really the only solution,” Howe said. “It’s a stopgap way to try and protect your privacy while also registering your dissatisfaction as a user to the Googles of the world.”