Culture
By Steven Rosenfeld / AlterNet
March 21, 2018

Facebook's Latest Data Breach Reveals Silicon Valley's Fortunes Are Built on Pilfering Privacy

Facebook has the keys to our personal lives. And that's just the beginning of the end of our privacy.

Mark Zuckerberg - Photo Credit: Screenshot / YouTube

One of the worst weeks in Facebook's history—its stock tumbled, Congress and Parliament demanded top executives testify and explain, and the Federal Trade Commission opened a new investigation—is due to a simple fact: the company shares and sells privacy-breaching profiles of millions of users.

Facebook's latest troubles rose to the top of the news this weekend when a series of investigative reports in the U.S. and Britain found that private political consulting firm Cambridge Analytica, created by Trump's former political guru Steve Bannon, had stolen 50 million Facebook user profiles. The profiles were intended to be used in the 2016 election for the electoral equivalent of psychological warfare: to push, prod, play on prejudices, you name it, and provoke millions of Americans in swing states to vote for Donald Trump—or not to vote for Hillary Clinton.

It turns out Trump's campaign didn't use Bannon's psychological warfare machine after all. Cambridge Analytica's data simply wasn't as good as Facebook's own customized advertising platforms, in conjunction with the Republican Party's voter files. Beyond that takeaway, to stop giving Bannon credit where it's not due, Facebook's problems stem from the fact that it's a privacy-busting social media platform.

But this feature, which some people find deeply disturbing, isn't unique in Silicon Valley. Rather, it is indicative of what's coming under the rapidly developing Internet of Things. That realization puts Facebook's latest political turmoil, and the various governmental responses, into an odd category: what's noisy today isn't likely to change what's coming tomorrow, as the loss of privacy is a given for the touted benefits of a wired world.

> "This is not a story about hacking or data breaches, but about Facebook's privacy policies," said Paul Resnick, a professor of Information at the Center for Social Media Responsibility at the University of Michigan. "Cambridge Analytica gathered some information about 30-50 million people, via a FB app, but it's not clear that it got very much about each person."

While Resnick noted that Facebook

> "tightened its privacy policies four years ago, so that apps now can gather even less information about a user's friends than they could then," there's plenty of current debate about whether those steps were meaningful or akin to sticking a proverbial finger in a leaky dike. (Facebook was under an FTC consent decree to enforce privacy protections, which led it to announce a new investigation Tuesday.)

> "Cambridge Analytica was basically using Facebook as it was designed: as an enormous and enormously valuable trove of data about people," Alex Shephard wrote in the New Republic, saying that Facebook, not Bannon's crew, was the "shady" actor. "Facebook's apparent indifference to Cambridge Analytica's malfeasance for the past two years is an acknowledgment of this basic reality. The occasional bad actor—and there have been several—is the price of the company's business model, which is to sell its users' data."

Sandy Parakilas, the "platform operations manager at Facebook responsible for policing data breaches by third-party software developers between 2011 and 2012," made much the same point in a Guardian report.

> "Parakilas, 38, who now works as a product manager for Uber, is particularly critical of Facebook's previous policy of allowing developers to access the personal data of friends of people who used apps on the platform, without the knowledge or express consent of those friends."

But academics and others who study social media, including the information gathering practices powering its lucrative advertising business, say that everybody using social media like Facebook should know their private lives are being mined for profit. Needless to say, most social media users are not thinking about that when sharing personal thoughts or taking part in some public political activity.

> "When someone violates your privacy for profit, like we're seeing with Facebook and Cambridge Analytica, it feels like you've been robbed," said Will Potter, professor of journalism at the University of Michigan and a noted civil liberties advocate. "But we have to remember that we gave Facebook the keys to our personal information. And it doesn't stop there."

Potter explained that social media users have signed away their rights to privacy by opening accounts in their names on these platforms.

> "Facebook is just one of many social media platforms aggregating our lives, and most users accept these companies' terms of use without having read them. Unless we hold these companies accountable, they will continue to dominate other aspects of our lives."

But Potter makes a larger point—one that casts whatever pending action the FTC may take in a diminished light: whatever fine they may levy will be a business expense and not impede Silicon Valley's evolving drive to monitor people's behaviors and tie in their digital devices to create a so-called Internet of Things.

> "In [Facebook CEO] Mark Zuckerberg's 'manifesto,' for instance, we should remember that he promised: 'We are committed to always doing better, even if that involves a worldwide voting system to give you more voice and control.' This data breach should put an end to any possibility of Facebook being used for voting, and it's an opportunity for all of us to rethink the trust we have put in social media companies."

Bigger Picture: Privacy Shrinks as the *Internet of Things* Grows

In 2014, *Pew Research* published a report describing how the *Internet of Things* will thrive by 2025 and discussed its promises, perils and unknowns. What it says about vanishing privacy and its personal and societal implications resonates with the latest *Facebook* brouhaha over 50 million user profiles being easily accessed and stolen.

> "Many experts say the rise of embedded and wearable computing will bring the next revolution in digital technology," the Pew summary began. "They say the upsides are enhanced health, convenience, productivity, safety and vastly more useful information for people and organizations. The downsides: challenges to personal privacy, over-hyped expectations, and tech complexity that boggles us."

JP Rangaswami, chief scientist for *Salesforce.com*, described what's coming:

> "The proliferation of sensors and actuators will continue," he said, referring to the many apps, devices and home appliances that are now commercially available. "'Everything' will become nodes on a network. The quality of real-time information that becomes available will take the guesswork out of much of capacity planning and decision-making."

But as *Pew's* report noted—and as Bannon's *Cambridge Analytica* boasted of doing, but failed to do in 2016—*the capitalists behind Silicon Valley's revolution want to deploy computing not just to sell things, but to provoke and change behavior*.

> "Many expect that a major driver of the Internet of Things will be incentives to try to get people to change their behavior—maybe to purchase a good, maybe to act in a more healthy or safe manner, maybe work differently, maybe to use public goods and services in more efficient ways," the report said. "Laurel Papworth, social media educator, explained, 'Every part of our life will be quantifiable, and eternal, and we will answer to the community for our decisions. For example, skipping the gym will have your gym shoes auto tweet (equivalent) to the peer-to-peer health insurance network that will decide to degrade your premiums. There is already a machine that can read brain activity, including desire, in front of advertising by near/proximity. I have no doubt that will be placed into the Big Data databases when evaluating hand gestures, body language, and space for presenting social objects for discussion/purchase/voting.'"

The specter of a disruptive digital Big Brother disturbs privacy advocates such as the Electronic Privacy Information Center, or EPIC, which for years has called on the FTC to pressure Facebook to abide by its 2011 consent decree—which the latest disclosures about Cambridge Analytica's theft of millions of user files appear to have flaunted.

Frank Pasquale, a law professor and EPIC advisory board member, told Pew's researcher that expansion of the Internet of Things will result in a world that is more

> "prison-like" with a "small class of 'watchers' and a much larger class of the experimented upon, the watched." In another article, he predicted the Internet of Things "will be a tool for other people to keep tabs on what the populace is doing."

While others offer less doomsday-ish scenarios, one impact is certain: privacy will vanish.

> "It [the Internet of Things] will have widespread beneficial effects, along with widespread negative effects," Justin Reich, a fellow at Harvard University's Berkman Center for Internet & Society, told Pew. "There will be conveniences and privacy violations. There will be new ways for people to connect, as well as new pathways towards isolation, misanthropy, and depression. I'm not sure that moving computers from people's pockets (smartphones) to people's hands or face will have the same level of impact that the smartphone has had, but things will trend in the similar direction. Everything that you love and hate about smartphones will be more so."

What's also clear is that different kinds of personal information—writings, speech and behavior—will also be tracked, Pew's experts said; often with unanticipated side effects or impacts.

> "The Internet of Things is too complex. It will break, over and over," said Jerry Michalski, founder of REX, the Relationship Economy eXpedition. "They will also be prone to unintended consequences: they will do things nobody designed for beforehand, most of which will be undesirable. We aren't evolved enough as a species or society to create apps and services that are useful to humanity in the Internet of Things. We'll try to create efficiencies but be thwarted by nature's complexity. False positives from contextual movements will break people's willingness to have devices track their expressions and thoughts. Try using speech recognition in a crowded room. Now, imagine that it is your thoughts being tracked, not merely speech. Google Glass has already attracted backlash, before a thousand people are in the world using it. [It was taken off the market and sold to the U.S. military, beta testers previously told AlterNet.] Our surveillance society feels oppressive, not liberating. No comfortable truce will be found between the privacy advocates and the 'screen everything' crowd."

Facebook's latest travails are resonating because it is a global social media platform with 2 billion users, that is being exposed as insufficiently protecting people's privacy. But its gathering of private information, data mining and synthesis is hardly unique in Silicon Valley.

If anything, *Facebook's* practices are in line with where Silicon Valley wants to take the world: toward an *Internet of Things* where everyone and everything are wired together, and where privacy, as it's now known, is disappearing.

❒ Steven Rosenfeld covers national political issues for AlterNet. He is the author of several books on elections, most recently Democracy Betrayed: How Superdelegates, Redistricting, Party Insiders, and the Electoral College Rigged the 2016 Election (March 2018, Hot Books).