Why your online data isn't safe

October 3 2018, by Christina Pazzanese

Credit: CC0 Public Domain

Until recently, the presumptive targets for massive data theft were considered to be companies that lacked sophisticated cybersecurity or didn't take the issue seriously enough.

But since late 2016, some of the biggest names in cutting-edge tech have

seen their most sensitive customer data—including the content of emails, credit card numbers, and cellphone numbers—fall into the hands of hackers, or in some cases shared such data with third parties without the consumers' knowledge or consent.

The list is getting long fast. Thieves downloaded information on 25 million U.S. Uber riders. The credit reporting agency Equifax had 143 million customer files stolen by hackers. Cambridge Analytica harvested data from at least 87 million Facebook users to target with political ads. This summer, Google admitted to Congress that app developers and others have access to users' Gmail. Data scientists found major security flaws in AT&T, T-Mobile, and Sprint phones that left customers exposed. And just last week, Facebook revealed its largest breach, with 50 million users affected. It said phone numbers supplied to Facebook by users for two-factor authentication security had been shared with advertisers.

With so many violations—and so few repercussions—senior executives from Google, Apple, Amazon, and Twitter, among other firms, were summoned before the Senate Committee on Commerce, Science, and Transportation last week to explain why data privacy breaches continue, and to discuss some remedies. Sen. John Thune (R., S.D.), the committee chairman, said it's no longer a question of whether there needs to be a federal law to protect consumer data privacy but "what shape the law should take." Another hearing is planned later this month.

Urs Gasser, LL.M. '03, is executive director of the Berkman Klein Center for Internet & Society at Harvard University and a professor of practice at Harvard Law School. His research and teaching focus on information law and policy, and he writes frequently about privacy, data protection, and the regulation of digital technology. Gasser discussed the state of data privacy with the Gazette via email and suggested what might be done to protect users from companies that profit from people's

data.

Q&A

GAZETTE: As someone who has been studying data privacy for a long time, are you surprised by this string of failures?

GASSER: What is perhaps most surprising is the frequency with which such privacy-relevant incidents now become public, as well as their prevalence and scale. In terms of the underlying causes and effectiveness of responses, it's important to analyze each incident separately. A data breach caused by external hackers is not the same problem and doesn't require the same countermeasures as privacy threats resulting from data-sharing agreements between an online platform and advertisers that are at the core of the business model. That being said, the effects in terms of user privacy might be quite similar. It is also noteworthy that the GDPR [European Union General Data Protection Regulation] addresses a broad range of data-privacy violations, and it will be interesting to see whether the Facebook breach in particular will trigger GDPR enforcement action.

GAZETTE: Many of the biggest technology companies continue either to allow or to fail to prevent their customers' data from falling into the hands of advertisers, app developers, and other third parties. Despite frequent promises of better privacy protections, little has changed. Why aren't these companies taking this more seriously?

GASSER: To be fair, companies have made important efforts to better protect user data through a broad range of measures, including privacy dashboards, enhanced privacy and security features, such as end-to-end encryption, upgrades to their privacy policies, and more. But there is indeed a deeper structural problem at the core of the privacy battles of our time that makes current efforts feel insufficient. Most of today's tech business models are based on targeted advertisement, which relies on collecting, sharing, and analyzing vast amounts of user data. Simply put, to really prioritize user privacy would also mean to compromise an underlying business model that has been very successful in economic terms and produced some of the wealthiest companies in the world.

GAZETTE: Lawmakers have called on tech companies to better secure their user information and have hinted that they may begin strictly regulating how data is handled if the companies don't shore up data security. Will Congress do anything soon to hold these companies accountable, and, if not, what would it take for the federal government to take real action?

GASSER: In the current political climate, I'm doubtful that anything dramatic—say, like GDPR—will happen at the federal level anytime soon. But we see a lot of consumer privacy activity at the state level. Consider the recent enactment of the California Consumer Privacy Act, which is likely to be very influential given its scope of application, or Vermont's data-broker legislation. Combined with the enhanced consumer protection agenda by many State A.G.s, that's where the action is until Congress comes up with something meaningful. And, of course, there's also the increased pressure coming from the European legislative and data-protection authorities, based on the new protections and instruments set forth by the GDPR. Some argue that there is a "market

for privacy" emerging that will provide incentives, particularly to privacy startups, to be more privacy-friendly.

GAZETTE: Is it time to declare the voluntary-privacy-policy era a failure and start treating these businesses like public utilities?

GASSER: I agree that the self-regulatory model has failed to provide adequate levels of consumer privacy protection in today's tech environment. Where to go from here is more difficult to say, though. Many privacy advocates point to the GDPR as a new gold standard. I'm more skeptical, as such an approach is deeply rooted in European values, culture, and political economy and cannot be transplanted in a "cut and paste" way. It also comes with some serious drawbacks, in terms of compliance costs, for instance. I think it's time to rethink data privacy more fundamentally. You can find some of my thoughts here. To introduce fiduciary duties for tech companies is another interesting new way to think about some of the structural problems mentioned before.

GAZETTE: Who's to blame for where we are now? Are users partly at fault for not making more of a fuss about privacy violations? Do most people understand how much of their information is in the hands of others, and how it's being used?

GASSER: I would agree that it's too simple to just blame the tech companies for the status quo. I think we need to look at the privacy crisis as an ecosystem-level problem, with many forces at play—technological, market, behavioral, and legal—and many actors involved, including users who often make privacy decisions based on incomplete information and with cognitive biases at play. That is why I argue in my

own work in favor of a more holistic approach to the future of privacy, which combines strong legal protections with digital literacy and educational efforts, next-gen privacy-enhancing technologies, and economic incentives for more privacy-friendly services, among other elements in the strategy, as opposed to putting my bets on GDPR-like laws alone. Such an approach would also include smarter user education and empowerment.

GAZETTE: People can't opt out of using Google, and won't decide not to have a cellphone, so what can people do to protect themselves?

GASSER: There are a number of online privacy check-ups available and a series of privacy self-help tools, including privacy browsers or VPNs [virtual private networks], to name just two. Some of them are provided by tech companies themselves, and some are offered by consumer organizations such as EPIC or EFF. I would very much recommend that people make use of these offerings, even if they are only tactical in the sense that they understandably can't address the structural root cause of the problem.

This story is published courtesy of the Harvard Gazette*, Harvard University's official newspaper. For additional university news, visit* Harvard.edu.

Provided by Harvard University

Citation: Why your online data isn't safe (2018, October 3) retrieved 25 April 2024 from https://phys.org/news/2018-10-online-isnt-safe.html