Testimony of Ashkan Soltani[1]
Independent Privacy Researcher and Consultant

United States Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

Hearing on:
Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks

Tuesday, June 19, 2018

Chairman Moran, Ranking Member Blumenthal, and distinguished members of the Subcommittee: Thank you for the opportunity to testify about the ongoing risks posed to consumer digital privacy and how to approach consumer data privacy going forward.

My name is Ashkan Soltani. I'm a technologist specializing in privacy, security, and behavioral economics with over 25 years of experience. I previously served as one of the first technologists at the Federal Trade Commission (FTC), and later as Chief Technologist under Chairwoman Ramirez. I also served a brief stint as a senior advisor to the Chief Technology Officer in the White House Office of Science and Technology Policy under President Obama.

For over a decade, I have researched and written on digital privacy and consumer expectations online. My work originated in my graduate research, *Knowprivacy*,[2] in which my team and I explained that although companies posted lengthy privacy policies online, consumers often had little real understanding of what those policies did, and how their data would be used once collected. More disturbingly, our research concluded that companies, including Facebook rarely followed their own stated policies.[3]

I had the honor of addressing this very committee in 2011 to describe "The State of Online Consumer Privacy."[4] During that hearing, I described the pervasiveness of online tracking, how "notice and choice" is ineffective, and the need for technical and regulatory interventions. Today, some seven years later, nearly all of what I said then still applies, if anything with much greater scale and urgency. While companies have grown in technical capability and ability to influence consumers' behaviors, the government has remained static, and has not brought its considerable resources to bear on this issue.

---

[1] My oral and written testimony today to the Committee represent my own personal views, and do not reflect the views of any of the organizations I have worked for in the past.
[2] KNOWPRIVACY, http://knowprivacy.org (last visited June 18, 2018).
[3] KNOWPRIVACY, *Site Profiles: Facebook*, http://knowprivacy.org/profiles/facebook (last visited June 18, 2018).
[4] Testimony of Ashkan Soltani, United States Senate Committee on Commerce, Science, and Transportation, Hearing on The State of Online Consumer Privacy (Mar. 16, 2011), https://www.commerce.senate.gov/public/_cache/files/f4645a61-b16e-4fa7-a18c-f0361268f356/F94C2CFDD06D91AE3A9E044F9D888E6E.soltani-testimony.pdf.

Today, online giants collect private information from laptops, tablets, smartphones, televisions, and whatever other gadgets they happen to devise and connect to the Internet. They measure not only what we do online, but connect it to what we see and buy in the real world.[5] And still, consumers have little actual understanding of what they provide and how it's used, nor has any meaningful regulation been introduce to balance this erosion of personal privacy.

Members of the Subcommittee: I cannot stress enough that Cambridge Analytica's theft of person information is not a new problem. It is neither novel nor limited to one bad actor—albeit a strikingly egregious example. This problem is endemic to the online ecosystem and creates real harm to every American who uses the Internet, including the honorable members of this Subcommittee and their colleagues.

Today, I will highlight for the committee three main points regarding digital privacy online generally and Facebook's practices specifically.

First, I will explain that "notice and choice," the current federal framework for online privacy, is grossly inadequate to protect consumers. Next, I will provide examples of some of the particularly harmful practices of Facebook, including their leading role in the behavioral advertising "race to the bottom;" their policy of "two steps forward, one step backward;"and how they do, in fact, effectively "sell" user data. Lastly, I will describe how behavioral advertising and the practices enabling it are at least as intrusive as activities already barred under federal law and I will suggest some steps for legislating in the federal space.

The Current Notice and Choice Framework Is Inadequate to Protect Consumers

The current privacy framework is one of notice and choice—a company must provide its users with information on its practices, and a user consents to those practices when using the company's site or service. The FTC's privacy enforcement authority is based entirely on this framework. However, in practice, this does nothing to protect users: it is well known that users neither read nor understand most company's privacy practices. Mr. Zuckerberg himself, testifying earlier this year in front of the joint Commerce and Judiciary Committees, admitted that he did not expect users to read lengthy, verbose privacy policies.[6] A recent panel of witnesses recently before the House Energy & Commerce Subcommittee on Digital Commerce and Consumer Protection also unanimously agreed that consumers do not have a "clear

[5] Maureen Morrison, *Facebook Links Actual Store Visits to Marketers' Ads and Sales*, AdAge (June 14, 2016), http://adage.com/article/digital/facebook-adds-store-visits-measurement-tools/304493.
[6] Kaleigh Rogers, *Zuckerberg Says People Don't Understand How Facebook Uses Their Data Because Privacy Policies Are Hard*, Vice (Apr. 10, 2018), https://motherboard.vice.com/en_us/article/mbx5py/zuckerberg-says-privacy-policies-too-long.

understanding" of the contents of privacy policies.[7] Compounding the harm, the FTC has made clear that under this framework, a practice is generally permissible so long as it is disclosed.

Even if users did actually read the privacy notices, they have no way—short of boycotting a service—to object to privacy practices they find overly intrusive. For the vast majority of services and devices, the user "choice" is whether to accept the practices and use the service or to object and not use it at all. While some claim that users additionally have the choice to use competing services, in reality there is not meaningful opportunity to do so. In the same testimony where he acknowledged that users do not read privacy policies, Zuckerberg was also unable to name a direct competitor to Facebook that provided the same suite of services.[8]

Indeed, in addition to being a social networking destination, Facebook is now the de facto method by which users log in to third-party applications, such as other social applications, dating applications, and social lending sites. Many applications and online features require or strongly suggest verification with a Facebook profile, significantly limiting the availability of web services for anyone who chooses to not have a Facebook page.

Facebook Leads A Race to the Bottom for Online Privacy

No other single company has done more to erode consumer privacy than Facebook. This is not simply a function of Facebook's cavalier treatment of the data of its own users, although those practices remain disturbing. Rather, Facebook's business practices have driven the entire online advertising industry to adopt increasingly invasive tracking practices in what amounts to a race to the bottom for privacy. To be sure, Facebook is responsible for moving the advertising goalposts from tracking based on pseudonyms and anonymous markers to tracking based on an individual's real names, age, and location.

This is not simply conjecture. It is widely acknowledged in the industry that the primary reason that then-Google CEO Larry Page tied all employee bonuses to "the success of Google's social strategy" and so hastily implemented their social network (Buzz) was to compete with the rapid growth of Facebook.[9] Buzz's implementation and data use subsequently landed Google under an FTC consent decree, wherein Google promised to maintain its privacy promises to consumers. However, even under FTC decree, Google has continued its behavioral tracking

---

[7] ENERGY & COMMERCE COMM., *Press Release: #SubDCCP Holds Hearing on Digital Advertising Ecosystem* (June 14, 2018), https://energycommerce.house.gov/news/press-release/subdccp-holds-hearing-on-digital-advertising-ecosystem ("Vice Chairman Adam Kinzinger (R-IL) posed an important question to our expert panel, 'Do any of you believe consumers have a clear understanding of what's contained in a privacy policy?' To which all four witnesses answered with a unanimous no.").

[8] Sarah Jeong, *Zuckerberg Struggles to Name a Single Facebook Competitor*, VERGE (Apr. 10, 2018), https://www.theverge.com/2018/4/10/17220934/facebook-monopoly-competitor-mark-zuckerberg-senate-hearing-lindsey-graham.

[9] *See* Nicholas Carlson, *Larry Page Just Tied All Employees' Bonuses to the Success of Google's Social Strategy*, BUS. INSIDER (Apr. 7, 2011), http://www.businessinsider.com/larry-page-just-tied-employee-bonuses-to-the-success-of-the-googles-social-strategy-2011-4.

with users' real identities to further erode the ability of users to engage online privately.[10] These industry-wide practices, led by Facebook, continue to substantially intrude into users' private lives and expose them to risk of exploitation and manipulation by corporate and government actions.

Facebook Employs a Privacy Policy of "Two Steps Forward, One Step Back"

To reiterate, nothing we have seen this year is new behavior from Facebook. As the principal technologist at the FTC responsible for investigating Facebook's practices, I saw that time and again, Facebook was engaged in unfair and deceptive practices. Specifically, in 2011, Facebook agreed to settle charges that it deceived consumers by, among other things:

> 1) narrowing its definition of privacy without notifying consumers, allowing previously private consumer information to be accessible to anyone on the web;
> 2) allowing apps to have sweeping access to user data after telling users that they could keep their information private from those apps;
> 3) telling users they could restrict sharing of data to limited audiences—for example with "Friends Only"—but in fact allowing sharing with third-party applications used by their friends;
> 4) claiming to verify the security of apps when it did not do so; and
> 5) retaining user information even after users deleted their accounts.[11]

These alleged practices, along with numerous other privacy infringements throughout the company's history, have led to few or no meaningful repercussions to Facebook's success.[12] For example, as an independent researcher, I demonstrated that Facebook was intercepting the contents of user conversations in order to detect references to other brands or websites.[13] It would then share information about those conversations with the operators of those pages or websites by reporting a "Like" from the user on the Facebook page—providing those third parties an open window into users' private conversations.[14] The latest Cambridge Analytica missteps by Facebook are only the latest in a series of bad actions taken by the company.

---

[10] Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, ProPublica (Oct. 21, 2016), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.
[11] Fed. Trade Comm'n, *Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
[12] Alyssa Newcomb, *A Timeline of Facebook's Privacy Issues—And Its Responses*, NBC (Mar. 24, 2018), https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651.
[13] Kashmir Hill, *Facebook Scans Private Messages to Hand Out Public 'Likes'*, Forbes (Oct. 4, 2012), https://www.forbes.com/sites/kashmirhill/2012/10/04/facebook-scans-private-messages-to-hand-out-public-likes/#735fb4fd2738.
[14] Wendy Davis, *Facebook Agrees to Settle Class-Action Over Message Scans*, MediaPost (Dec. 23, 2016), https://www.mediapost.com/publications/article/291771/facebook-agrees-to-settle-class-action-over-messag.html.

Facebook Leverages Its Control of Consumer Information for Growth in Market Share

Facebook is the custodian of user information, and it allows its commercial partners access to that data in exchange for growth and expansion opportunities. Recent reporting by the *New York Times* detailed Facebook's practice of giving certain device maker partners privileged access to the platform and allowing those partners to override users' privacy controls without notifying affected users.[15] I was provided one of these "privileged access tokens" by the reporters investigating the story and personally tested this functionality. With it, I was able to view vast amounts of information about a user's friends by simply emulating the access given to the privileged partner—access which allowed me to override the user's chosen platform privacy settings that would normally block these types of third parties from accessing their information.[16]

Follow-up reporting by the *Wall Street Journal* confirmed that in addition to hardware makers, certain Facebook "platform partners" (i.e. website and app developers) were also provided privileged access to users' private information.[17] There is quite a bit of confusion about the exact details reported,[18] but my understanding is that while in April 2014, Facebook announced that it would not allow app developers to access certain information (such as information about a user's friends), it did not enforce this policy until one year after the announcement—in May 2015. When that time came around, however, Facebook selectively granted extensions to certain of its more prominent advertisers, included a major automotive company and a large Canadian bank.

These types of "privacy for sale" walkbacks are par for the course. For example, in response to the current Cambridge Analytica scandal, Facebook initially sought to banish all data brokers from the platform. However, Facebook "quickly softened its stance after big marketers threatened to pull their ad dollars" from the platform.[19]

While Facebook claims it does not sell user data to advertisers,[20] it commodifies this data and brokers access to consumer information to achieve unparalleled growth and dominance online.

---

[15] Gabriel J.X. Dance, et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N. Y. Times (June 3, 2018), https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html.

[16] For example, the access token that was granted to me by the *Times* allowed me to access information on the reporter's friends—overriding the friend's privacy settings. *See* @ashk4n, Twitter (June 4, 2018, 8:19 AM), https://twitter.com/ashk4n/status/1003657433770811393.

[17] Deepa Seetharaman & Kirsten Grind, *Facebook Gave Some Companies Special Access to Additional Data About Users' Friends*, Wall St. J. (June 8, 2018), https://www.wsj.com/articles/facebook-gave-some-companies-access-to-additional-data-about-users-friends-1528490406.

[18] @facebook, Twitter (June 8, 2018, 4:34 PM), https://twitter.com/facebook/status/1005231609619021827?s=21.

[19] Joel Schectman, *Facebook Releases New Privacy Safeguards After Ceding to Pressure from Advertisers*, Reuters (June 13, 2018), https://www.reuters.com/article/us-facebook-privacy-broker/facebook-releases-new-privacy-safeguards-after-ceding-to-pressure-from-advertisers-idUSKBN1J924P.

[20] Jordan Crook, *Mark Zuckerberg: "We Do Not Sell Data to Advertisers"*, TechCrunch (Apr. 10, 2018), https://techcrunch.com/2018/04/10/mark-zuckerberg-we-do-not-sell-data-to-advertisers.

While many view Facebook as a two-sided marketplace—connecting consumers and advertisers—in fact, it also services a crucial third market. In order to thrive, Facebook must attract developers, who create new apps and features for Facebook akin to a traditional "Channel Partner" in sales.[21] Rather than directly paying in currency, Facebook reimburses them "in kind" with access to consumer information—often much more than necessary to create a functional service on the website and often for great benefit to the developers.

So, rather than selling data outright, the company instead rewards developers with broad access to consumer's information via its Application Programming Interface (APIs) and other integration tools. Those developers then create third-party applications or plug-ins that allow Facebook to thrive and spread across the web. This model allows Facebook to dominate, as users quickly realize that to use other basic web services they must use Facebook as a way to log-in.[22] Facebook treats these developers as major stakeholders in the business, and provided them with incredible access with little or no oversight. As Facebook employee 51, Katherine Losse explains, Facebook treated developers as trusted insiders, courting them with parties and "look[ing] away from the fact that almost all of Facebook users' data was available to them through the platform. Technically, [the developers] were supposed to scrub their servers of the data every twenty-four hours but, if they didn't, we had no way of knowing. Mark [Zuckerberg] implicitly trusted developers."[23]

The business model of rewarding developers with private user data and refusing to take even basic steps to protect that information from abuse is exactly what has put users directly in the line of fire in this latest Facebook privacy lapse. The larger harmful effects of this model should not be overlooked. "Growth at any cost" is the new "unsafe at any speed," and must be treated as such.

Behavioral Profiling Can Be as Invasive as Wiretapping

Perhaps the clearest comparison that can be drawn about the invasiveness of Facebook's insights is one to the physical world. One need not look further than the rash of stories surrounding Facebook's purported access of smartphone microphones and cameras. Time and again,[24] individuals make allegations that Facebook surreptitiously monitored them through a smartphone's microphone or camera in order to eavesdrop on conversations and target them

[21] A channel partner typically partners with a company to co-brand or co-develop technologies or new products.
[22] Amanda Schupak, *What Are You Sharing When You Sign In with Facebook or Google?*, CBS (Nov. 3, 2015), https://www.cbsnews.com/news/what-are-you-sharing-when-you-sign-in-with-facebook-or-google.
[23] Katherine Losse, The Boy Kings: A Journey Into the Heart of the Social Network (Free Press 2012).
[24] *See* Joanna Stern, *Why It Feels Like Facebook Is Listening Through Your Mic*, Wall St. J. (Mar. 7, 2018), https://www.wsj.com/video/series/joanna-stern-personal-technology/why-it-feels-like-facebook-is-listening-through-your-mic/AAB3CF21-F765-4C6A-920A-FB2DA950288E; *Is Your Phone Listening In? Your Stories*, BBC News (Oct. 30, 2017), https://www.bbc.com/news/technology-41802282.

with advertisements based on those discussions. These users believe this because the inferences made by Facebook and advertisers are so deeply intimate that the individuals conclude that those inferences could only be made by monitoring the private conversations of those individuals. To be clear, I and other researchers have found little evidence to support claims of Facebook surreptitiously accessing users' microphones. Despite this, the claims themselves shed a light into how invasive behavioral inferences can be, and the visceral response users have to the monitoring they are subjected to by Facebook and its partners.

Congress and the legal system are no strangers to protecting private information when it is monitored by phone or camera. Our society has long recognized that an individual has a right to private communication and a right to be left alone. We have taken great strides to advance those rights and protect them when new technology threatens to infringe. Now is such a time, and federal action is required. Protecting privacy is now more critical than ever.

Federal Regulation is Necessary to Prevent Future Harms

So what can be done to protect digital privacy online? "Privacy" as a concept can no longer be considered simply as the individual right to prevent the publication of private information or to keep prying eyes out of one's home. We now live in a world where our most private details—conversations with friends, romantic preferences, and financial information—reside by necessity with online companies. Those companies then use that data to market to and sell the ability to target citizens based on those traits. The same tools can also be used to influence our perception of the world around us and influence our decisions therein, such as when Russia took active steps to sow propaganda in America to create discord in our recent political cycle.

We've seen the harmful effects of the erosion of user privacy, and can no longer simply content ourselves with imagining this debate as a squabble between privacy advocates and online data companies. The rules on what private information can be collected, how it can be used, and by whom it can be used have enormous impacts on the wellbeing of large swaths of society, and indeed, on the legitimacy of our democracy writ large.

The government must take meaningful action to prevent Facebook and other Internet giants from causing lasting harm to American discourse and democracy. The FTC has called repeatedly for an omnibus privacy regulation that would give it meaningful authority to set appropriate rules of the road for consumers online. That authority would provide a real step forward in providing flexible, fair rules that respect both business needs and consumer vulnerability.

Any federal legislation should aim to address many of the key problems facing consumers online: lack of meaningful consent, inadequate data security practices, and a lack of any real transparency from large online companies. These issues arise time and again, and have

spurred action at the state level, such as with the California Consumer Privacy Act,[25] a ballot initiative I helped to write. That initiative, and others like it,[26] might well provide the state-level experimentation necessary to create meaningful federal policy in Washington.

I thank you for your time, and look forward to answering any questions you might have.

[25] CA. CONSUMER PRIVACY ACT, https://www.caprivacy.org (last visited June 18, 2018).
[26] NAT'L CONF. STATE LEGS., *Privacy Legislation Related to Internet Service Providers—2018*, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx (last visited June 18, 2018).