AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–889

CAMBRIDGE ANALYTICA AND OTHER FACEBOOK PARTNERS: EXAMINING DATA PRIVACY RISKS

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION,
PRODUCT SAFETY, INSURANCE,
AND DATA SECURITY

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 19, 2018

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
58–439 PDF WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi	BILL NELSON, Florida, *Ranking*
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	RICHARD BLUMENTHAL, Connecticut
JERRY MORAN, Kansas	BRIAN SCHATZ, Hawaii
DAN SULLIVAN, Alaska	EDWARD MARKEY, Massachusetts
DEAN HELLER, Nevada	TOM UDALL, New Mexico
JAMES INHOFE, Oklahoma	GARY PETERS, Michigan
MIKE LEE, Utah	TAMMY BALDWIN, Wisconsin
RON JOHNSON, Wisconsin	TAMMY DUCKWORTH, Illinois
SHELLEY MOORE CAPITO, West Virginia	MAGGIE HASSAN, New Hampshire
CORY GARDNER, Colorado	CATHERINE CORTEZ MASTO, Nevada
TODD YOUNG, Indiana	JON TESTER, Montana

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY

JERRY MORAN, Kansas, *Chairman*	RICHARD BLUMENTHAL, Connecticut, *Ranking*
ROY BLUNT, Missouri	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	EDWARD MARKEY, Massachusetts
DEB FISCHER, Nebraska	TOM UDALL, New Mexico
DEAN HELLER, Nevada	TAMMY DUCKWORTH, Illinois
JAMES INHOFE, Oklahoma	MAGGIE HASSAN, New Hampshire
MIKE LEE, Utah	CATHERINE CORTEZ MASTO, Nevada
SHELLEY MOORE CAPITO, West Virginia	
TODD YOUNG, Indiana	

CONTENTS

WITNESSES

APPENDIX

CAMBRIDGE ANALYTICA AND OTHER FACEBOOK PARTNERS: EXAMINING DATA PRIVACY RISKS

TUESDAY, JUNE 19, 2018

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3:05 p.m., in room SH–216, Hart Senate Office Building, Hon. Jerry Moran, Chairman of the Subcommittee, presiding.

Present: Senators Moran [presiding], Thune, Fischer, Young, Blumenthal, Klobuchar, Markey, Udall, Hassan, and Cortez Masto.

OPENING STATEMENT OF HON. JERRY MORAN, U.S. SENATOR FROM KANSAS

Senator MORAN. Welcome to our Consumer Protection, Product Safety, Insurance, and Data Security Subcommittee hearing on Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks.

Earlier this year, reports surfaced regarding a personality-test application called "This is Your Digital Life," founded in 2014, that was hosted on Facebook and downloaded by approximately 300,000 Facebook users, who consented to the collection of data from their profiles. However, Facebook rules for third-party applications at that time allowed users to consent on behalf of their Facebook friends for their profile information to be collected also. This arrangement allowed this application to collect data from tens of millions of Facebook users by getting an affirmative consent of only 300,000 users. The application also shared this information with a data analytics firm called Cambridge Analytica, which worked with political campaigns on targeted advertising. It is alleged that other applications participated in similar collection practices, but Facebook changed their terms of service to prohibit this practice in 2015.

While Facebook sought assurances from Cambridge Analytica and developers of personality-test application that the user data in question was deleted, media reports earlier this year indicated they were not. Following the calls of concern from Congress and public alike, the Federal Trade Commission confirmed in March that the agency was investigating the privacy practices of Facebook and the company's compliance with the consent order issued by the FTC in

July 2012 to resolve allegations that the firm violated FTC Act, which prohibits deceptive and unfair practices affecting commerce.

There have since been additional consumer protection concerns flagged against Facebook, including reports that, over the last decade, Facebook established partnerships, called Application Programming Interfaces, with approximately 60 mobile device manufacturers in an effort to provide private data channels for those manufacturers. While Facebook has since provided some clarity on the purpose of these partnerships, outstanding questions remain regarding the role of Chinese telecommunication manufacturers.

This hearing follows a joint hearing between the full Senate Commerce Committee and the Senate Judiciary Committee in which we heard from CEO and Chairman of Facebook, Mark Zuckerberg, the company's data collection and sharing arrangements with third parties and how its user privacy is safeguarded. Additionally, I coauthored letters with my colleagues, Chairman Thune and Senator Wicker, to Facebook and Strategic Communication Laboratories, the British parent company of Cambridge Analytica, to provide answers to their specific dealings with one another related to consumer data.

My goal today is to hear from subject-matter experts in the use of social media data for commercial, political, and research purposes, the examination of the state of research surrounding social media data and targeted advertising that's critical to enabling this Subcommittee to better identify necessary steps to protect consumers.

It is my pleasure to introduce our expert panel today. As I've indicated previously, thank you all for your willingness to be here.

Mr. John Battelle is the Chief Executive Officer of NewCo and a member of the Board of Directors of Acxiom Corporation, a data broker company that formerly partnered with Facebook. He also founded *Wired* magazine and authored the international bestseller of "The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture in 2005."

Dr. Aleksandr Kogan is Lecturer at the Department of Psychology at the University of Cambridge, who designed the controversial personality-test app that collected user data of Facebook's consenting users and their friends. Facebook alleges that he violated their policies by sharing information with Cambridge Analytica, and his testimony will provide additional perspective for the Subcommittee's consideration related to the recent scandal.

Mr. Ashkun Soltani is a technology expert with Soltani LLC. With more than 20 years of experience as a consultant and researcher focused on technology, privacy, and behavioral economics, he served as a technical expert to a number of consumer protection agencies, including the FTC and State's Attorney General. He recently served as the chief technologist of the FTC, where he led a number of investigations into technology and Internet companies.

Additionally, David Sumpter, a professor of mathematics at Uppsala University in Sweden, has analyzed some of these issues related to Cambridge Analytica's scandal. Although he could not appear today, he has submitted written testimony for the record titled "Why the Facebook Data Available to Cambridge Analytica

Could Not Be Used to Target Personalities in the United States Presidential Election."

I ask unanimous consent that his testimony be admitted into the record. Without objection.

[The information referred to follows:]

WHY THE FACEBOOK DATA AVAILABLE TO CAMBRIDGE ANALYTICA COULD NOT BE USED TO TARGET PERSONALITIES IN THE U.S. PRESIDENTIAL ELECTION

Professor David Sumpter [1]

In this testimony I focus on the statistical approach I took to whether the psychological targeting that rose to prominence with the Cambridge Analytica affair could actually work. This document is adapted from the book *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles—The Algorithms That Control Our Lives (featuring Cambridge Analytica),* Bloomsbury, 2018.

During 2017 I investigated the use of Facebook to predict personalities. My interest in this area arose, when after the 2016 U.S. presidential election, Cambridge Analytica announced that its data-driven campaign had been instrumental in Donald Trump's victory.

Cambridge Analytica (CA) gave a great deal of prominence to personality algorithms in its promotional material. When CEO Alexander Nix presented his company's research at the Concordia Summit in 2016,[2] he talked about how, instead of targeting people on the basis of socio-economic background, as Barack Obama had done in his campaign, CA could "predict the personality of every single adult in the United States of America". Highly neurotic and conscientious voters were targeted with the message that the "second amendment was an insurance policy". Traditional, agreeable voters were told about how "the right to bear arms was important to hand down from father to son". He claimed that he could use 'hundreds and thousands of individual data points on audiences to understand exactly which messages are going to appeal to which audiences'.

When the story that Cambridge Analytica had been using data collected from Facebook users broke, in March 2018, most of the details of the "data breach", as Facebook later described it, were in fact already known inside the industry. I had knowledge of how the data was downloaded, having interviewed Alex Kogan, the Cambridge University researcher who had created the app that was used to conduct personality tests on 200,000 Facebook users. For a few dollars each the participants had answered personality questions and given permission for their own and their friends' Facebook profiles to be downloaded. Kogan's intention was to use this data to model personalities using Facebook data, enabling Alexander Nix to carry out his plan.

Kogan had been attempting to replicate the work of his colleague Michal Kosinski, who as a PhD student in Cambridge had collected an even bigger data set of the online personalities. Using an App called myPersonality, over three million people gave Kosinski and his colleagues permission to access and store their Facebook profiles. Many of these people then took a battery of psychometric tests, measuring intelligence, personality and happiness, and answered questions about sexual orientation, drug use and other aspects of their lifestyle. Michal Kosinski used this data to show that the, so called, Big Five personality traits—openness, conscientiousness, extroversion, agreeableness and neuroticism—could be predicted by the 'likeswe make on Facebook. He found that outgoing people on Facebook like dancing, theatre and *Beer Pong;* shy people like *anime,* role-playing games and Terry Pratchett books; neurotic people like Kurt Cobain, emo music and say "sometimes I hate myself"; and calm people like skydiving, football and business administration.

Kosinski used a statistical technique known as regression to convert the "likes" people had made on Facebook in to numerical predictions about their personality and political persuasion. This was the basis of the "psychological warfare tool", a term later used by whistleblower Chris Wylie, that Nix had described at the Concordia summit.

I was sceptical, both by the claims made by Alexander Nix and Chris Wylie and decided to test them for myself as part of the writing of my book *Outnumbered.* I

[1] Mathematics Department
Uppsala University
Box 480
75106 Uppsala Sweden

[2] See: *https://www.youtube.com/watch?v=n8Dd5aVXLCc*

don't have access to the data downloaded by Kogan, but Kosinski and his colleagues have created a tutorial package to allow psychology students to practise creating regression models on an anonymized database Facebook users.[3] The full data set contains data of the results of personality tests taken by 110,728 U.S.-based Facebook users, classifying them on five dimensions of Openness, Contentiousness, Extraversion, Agreeableness and Neuroticism (the so-called OCEAN model). It also contains the Facebook likes of these people, which were spread over 1.5 million different like categories.

Many of the users didn't make many "likes", so following the suggestion in Kosinki's article I studied data on those who had made more than 50 likes. This comprised 19,742 users.

It is important to note that while 110,728 is smaller than the headline figure of 30 million Facebook users downloaded in the "data breach" this 30 million is a friends-of-friends calculation. In Kogan's study, at most, 200,000 people took personality tests. Thus the data set I analyzed is roughly half the size, and about the same quality as that which Cambridge Analytica had access to.

I now ask a series of questions. In what follows I am replicating part of the work in several articles written by Kosinski and his colleagues. But I am focusing on the specific question of whether this data would have been useful for targeting personalities in a political campaign.

1. Can we predict political leanings from "likes"

Only 4,744 of the 19,742 U.S.-based Facebook users in the dataset expressed a preference for either Democrats or Republicans. Of these, 31 per cent were Republicans. Democrats were, at the time the data was collected between 2007 and 2012, over-represented on Facebook. I used the data to fit a regression model with likes as inputs and then tested the model's performance in predicting political personality.

A good way to test the accuracy of a regression model is to pick two people at random, one Democrat and one Republican, and ask the model to predict which of the pair is the Republican from their Facebook pro le. This is an intuitive measure of accuracy. Imagine you met these two people, and you were allowed to ask them a few questions about their tastes and hobbies, after which you had to decide which person supported which political party. How often do you think you would get it right?

The accuracy of a regression model based on Facebook data is very good. In eight out of nine attempts, the regression correctly identifies the political views of the Facebook user. The main group of likes that identify a Democrat were for Barack and Michelle Obama, National Public Radio, TED Talks, Harry Potter, the I F—ing Love Science webpage and liberal current a airs shows like *The Colbert Report* and *The Daily Show*. Republicans like George W. Bush, the Bible, country and western music, and camping. These results are consistent with those reported in Kosinski's own research.[4]

It isn't too surprising that Democrats like the Obamas and *The Colbert Report* or that many Republicans like George W. Bush and the Bible. So I tried to see if I could break the regression model by taking some of the obvious "likes" out of the model and performing a new regression. The model still worked with 85 per cent accuracy, only a slight reduction in performance. Now it used combinations of likes to determine political affiliations. For example, someone who liked Lady Gaga, Starbucks and country music was more likely to be a Republican, but a Lady Gaga fan who also liked Alicia Keys and Harry Potter was more likely to be a Democrat. This is where the multiple dimensional understanding gained by using lots of "likes" produces unexpected and useful results.

This type of information could be very useful to a political party. Instead of Democrats focusing a campaign purely around traditional liberal media, they could focus on getting the vote out among Harry Potter fans. Republicans could target people who drink Starbucks coffee and people who go camping. Lady Gaga fans should be treated with caution by both sides. Although it is difficult to make a direct comparison, the accuracy of a Facebook-based regression model seems to beat traditional

---

[3] This data was until recently available at *https://sites.google.com/michalkosinski.com/mypersonality* It has now been removed and is no longer available for research or teaching purposes. Further details can be found in the article: Kosinski, Michal, Yilun Wang, Himabindu Lakkaraju, and Jure Leskovec. "Mining big data to extract patterns and predict real-life outcomes." *Psychological methods* 21, no. 4 (2016): 493.

[4] Kosinski, Michal, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behavior." *Proceedings of the National Academy of Sciences* 110, no. 15 (2013): 5802–5805.

methods that use demographics, such as age, gender and socio-economic background.

There are limitations, though. First of all, there is a fundamental limitation of statistical models. Remember, the output of algorithms isn't perfect. We can't expect a model to reveal your political views with 100 per cent certainty. While regression models work very well for hardcore Democrats and Republicans—as I established earlier, the accuracy is around 85 per cent—predictions about these voters are not particularly useful in a political campaign. Known party supporters' votes are more or less guaranteed, and they don't need to be targeted. In fact, the regression model I fitted to Facebook data does not reveal anything about the 76 per cent of people who didn't register their political allegiance. While the data shows us that Democrats tend to like Harry Potter, it doesn't necessarily tell us that other Harry Potter fans like the Democrats. This is the classic problem inherent to all statistical analyses; of potentially confusing correlation with causation.

A second limitation relates to the number of "likes" needed to make predictions. The regression model only works when a person has made more than 50 "likes" and, to make really reliable predictions, a few hundred 'likes' are required. In the Facebook data set, only 18 per cent of users "liked" more than 50 sites. After this data was collected, Facebook has succeeded in increasing the number of sites its users 'like', precisely so that it can better target advertising. But there are still a lot of people who don't 'like' very much on Facebook.

2. Can we predict personality from "likes"

The idea Nix describes in the video is that of targeting our political personalities. The question is: can an algorithm reliably identify neurotic or compassionate people from their 'likes'? The data set provided in Kosinski's tutorial included the results of a personality test that measured the Big Five traits [5] (Openness, Contentiousness, Extraversion, Agreeableness and Neuroticism). I followed the methodology proposed by Kosinski and used principal component analysis and linear regression to link between personality scores and Facebook "likes".

Konsinski and his colleagues work found a correlation between certain Facebook likes and the five personality traits. The Pearson correlation coefficient for the relationship between the five traits and likes were Openness (0.43), Contentiousness (0.29), Extraversion (0.4), Agreeableness (0.3) and Neuroticism (0.3). These are low, but statistically significant correlations. The question is what they mean in practice?

To give an idea of the strength of these relationships Figure 1 shows, for 100 people (form the Kosinski data set), how their personality score correlates from a questionnaire with their personality predicted by Facebook measured likes.

[5] A guide to personality testing can be found here: *https://ipip.ori.org*

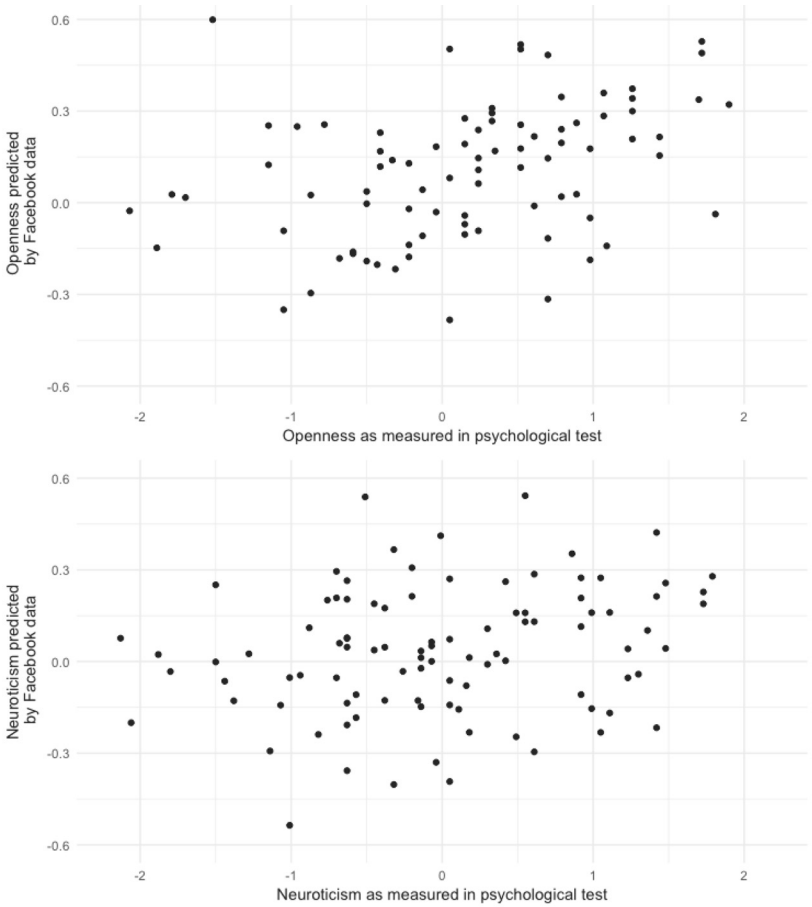

Figure 1: Illustration of the strength of the correlation between personality questionaire scores and Facebook-data predictions. Each dot is an individual from the data set collected by Kosinski and colleagues. Only 100 individuals are shown in the subsample, but data is selected so as to show same correlation as in the data as a whole. (Top panel) Correlation between a psychological test measure of openness and a prediction from Facebook data of openness (r=0.45), (Bottom panel) Correlation between a psychological test measure of neuroticism and a prediction from Facebook data of neuroticism (r=0.29).

Correlations are a scientific valid way of measuring connections, but they leave a lot to be desired when it comes to communicating how well a model performs.

I asked a different question of the same data: can it reliably be used for identifying neurotic individuals. I did a different statistical test, which is more relevant to the goals set out by Nix and those described by Chris Wylie. In my test, I repeatedly picked two people from the data set at random and looked at their neuroticism scores from the personality test they had performed. I compared these scores to a regression model based on Facebook 'likes'. The personality test and the regression model produced the same rankings for these pairs in around 60 per cent of cases. If I had set scores at random, I would have been correct 50 per cent of the time. The model was only slightly better than random.

The regression model was a bit better at classifying people in terms of their openness: it was correct about 67 percent of the time. But when I performed the same test on extroversion, conscientiousness and agreeableness I got similar results as for neuroticism: the model got it right about 58 percent to 63 percent of the time.

In summary, the accuracy of the models is too low, to psychologically profile individuals and target them during an election. A campaign based on this approach

would, in many cases, misidentify neurotic people, for example, and target them with the wrong advert.

One question that is often raised in objection to my argument above relates to how only a small difference in voter behaviour is needed to swing an election like the U.S. presidential election. The point made is that although 60 percent isn't much more than 50 percent, the increase in effectiveness could be crucial. The last election was won by a small margin.

This argument does not hold up to closer scrutiny. In the US, both sides spend vast quantities of money during a presidential election. The important point to consider is about how effective the various methods employed by the campaigns are in getting their message across. There *are* effective methods for communicating in the media, such as viral videos that everyone sees and talks about, political rallies and stories in the traditional media. These are likely to be much more effective than trying to identify personalities.

A further problem with 'personality algorithms' lies in how they can be applied. The neuroticism of Kurt Cobain fans, identified by Kosinski's work, is very different from the neuroticism of a gun owner set on protecting his family, that Nix envisaged targeting in advertising campaigns. Showing an advert about the second amendment to a Nirvana fan may well prove counterproductive.

Taken together, these limitations make it all but impossible to create a tool for identifying and manipulating us psychologically in the way envisaged in Nix original presentation. When I spoke to Alex Kogan he confirmed that he had, independently, reached similar conclusions to my own after working with the data he collected. His work with Cambridge Analytica didn't work. Nix has since reversed his position telling the UK houses of parliament committee in May that the approach had proved fruitless.

There is an important distinction to be made here between a scientific finding—that a certain set of 'likes' on Facebook is related to the outcome of personality tests—and the implementation of a reliable algorithm based on this finding, creating an equation that correctly predicts what type of person you are. A scientific finding can be true and interesting, but unless the relationship is very strong (which it isn't in the case of personality prediction) it doesn't allow us to make particularly reliable predictions about an individual's behaviour.

Conclusion

One reason that the distinction between scientific results and applied algorithms became blurred, both (apparently) in Alexander Nix mind and in our public consciousness, lies in the way results like this are reported in the media. In January 2015, *Wired* magazine wrote an article titled: "How Facebook knows you better than your friends do". The *Telegraph* newspaper in the UK went one step further and ran the headline: "Facebook knows you better than your [sic] members of your own family". Not to be outdone, the *New York Times* topped all other media outlets by going with: "Facebook knows you better than anyone else".

All of these headlines were followed by a report on a scientific article published by Michal Kosinski looking at how well Facebook "likes" predicted answers to personality questions, but this time, compared a regression model based on likes to answers from a 10-item questionnaire that work colleagues, friends, relatives and partners filled in about the Facebook user. The scientific result, which the newspapers were attempting to capture in their various headlines, was that their statistical model correlated better with the personality test than the 10 answers made by friends and family.[6]

Brian Connelly, associate professor at the Department of Management at the University of Toronto, Scarborough, who studies personality in the workplace, what he thought about this. "Michal [Kosinski]'s work is interesting and provocative, but I think the media are sensationalising the findings," he told me. "A more appropriate headline like, 'Preliminary findings suggest that Facebook knows some of you about as well as a close acquaintance (but we're holding out to see whether Facebook can predict your behaviour)', isn't very splashy." Brian's revised headline sums it up. The science is interesting, but there is no evidence yet that Facebook can determine and target your political personality.

---

[6] Youyou, Wu, Michal Kosinski, and David Stillwell. "Computer-based personality judgments are more accurate than those made by humans." *Proceedings of the National Academy of Sciences* 112, no. 4 (2015): 1036–1040.

During my research and writing of Outnumbered,[7] I found that newspaper articles and headlines often fail to reflect what algorithms can and can't do. I also looked at the role of Facebook in controlling the news we see, the role of fake news in the U.S. election, the question of whether automated bots on Twitter and other platforms are influential and the claims of general artificial intelligence. Often a more careful dissection of the algorithms reveals that the risks are exaggerated.

There is no general rule for the danger of algorithms. While many online algorithms have caused unnecessary scares, the use of algorithms in credit scoring, sentencing decisions and job ratings are causing problems. Cathy O'Neil argues this point convincingly in her book "Weapons of Math Destruction".[8] Usually the problems arise because algorithms used to classify us make mistakes or are interpreted incorrectly. That is exactly what happened in the case of Cambridge Analytica.

Senator MORAN. I look forward to hearing the testimonies of these expert witnesses, but now I turn to my colleague—well, I guess I look forward to hearing your words, as well—I now turn to my colleague, the Ranking Member, Senator Blumenthal, of Connecticut.

STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you, Senator Moran. And my thanks to you for your leadership in having this hearing, and to our witnesses for being here.

One of the central challenges of our time is becoming the potential threats posed by the Internet, such as data brokers, terrorist recruitment, Russia's continued interference in our elections. These challenges and threats are combined with the enormous promise and potential boons of the Internet. We've seen, for example, two Facebooks. One is the idealistic technology company driven by altruistic purpose to connect people with people they love, voices that need to be heard, communities that can be built. The other Facebook is an Internet behemoth that is one of the most powerful social and political tools in history, building pervasive data collection. And this Facebook is largely hidden to the public. One of our challenges is to reveal it fully and the way that it is using private confidential information—in fact, monetizing it—for its own self-purposes.

The discussion has been prompted, today, by the actions of Cambridge Analytica, a firm that sought to build pervasive and invasive psychological profiles to manipulate voters based on sensitive information. One initiative was the harvesting of Facebook data in which Cambridge Analytica found a willing partner in Professor Kogan. Facebook's failure of oversight meant that Professor Kogan could create an app to collect not only the personal data of hundreds of thousands that installed the app, but tens of millions of their friends.

I have been frustrated by Facebook's apparent reluctance to be more transparent to the American public about what it knows, where it acquires information, and what it uses it for. Facebook users are led to believe that the company's knowledge about them is limited to what they share, pictures of pets, messages wishing

[7] Sumpter, David. *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles—The Algorithms That Control Our Lives (featuring Cambridge Analytica),* Bloomsbury 2018.

[8] O'Neil, Cathy. *Weapons of math destruction: How big data increases inequality and threatens democracy.* Broadway Books, 2016.

a Happy Father's Day. Instead, as we know and learn more about Facebook's data collection practices, clearly we are seeing how it is only providing the tip of the iceberg. An example is Facebook's previous partnerships with data brokers, which sought to collect information users would not provide on intimate aspects of people's lives: race, religion, educational level, and income.

During this hearing, we're going to be exploring the scale and impact of Facebook's data collection tactics. How does Facebook use its reach to intimately monitor its users for commercial gain? How is sensitive information, such as race and religion, used to manipulate the public?

Facebook has been embarked on an apology tour, but, in fact, it is reaching a turning point. It must be totally transparent and responsible to the public and its users, or it can commit to its continued course of nontransparency. And my hope is that Facebook will be more forthcoming, that we will expose, through these hearings, the full range of its activities that may infringe on privacy, and that the hearing about privacy risks will also alert the public to how their information can be shared and sold without their knowledge and consent.

I will be introducing a bill that will, in effect, provide a privacy bill of rights based, in part, on the standards that Europe has already adopted. Americans deserve no less privacy than European. And the way to begin this course forward, the path ahead, is by alerting the American public to what those threats and challenges are to their privacy, as well as the potential threats to our national security from Russian interference in our election, and other uses of the Internet that may be known to companies like Facebook, but not to the broad range of Americans.

So, this hearing is just another step. And I am thankful to Senator Moran for enabling this step, and to our Chairman, Senator Thune, for enabling both of us to pursue these very important issues.

Thank you, Mr. Chairman.

Senator MORAN. Thank you, Senator Blumenthal.

We'll now hear from our witnesses. And we will begin with Mr. John Battelle.

STATEMENT OF JOHN BATTELLE, CHIEF EXECUTIVE OFFICER, NEWCO

Mr. BATTELLE. Thank you, honorable Committee Members. I appreciate the opportunity to submit testimony to your Committee.

In the past 5 years, Facebook has come to dominate the public square, the metaphorical space where our society comes together to communicate with itself, to debate matters of public interest, and to privately converse. As a publisher, myself, I became increasingly concerned that Facebook's appropriation of public discourse would imperil the viability of independent publishers and cause the kinds of externalities with which we now struggle.

Facebook employed two crucial strategies to grow its service in the early days. The first is the newsfeed, which mixed personal news from friends with public stories from independent publishers. The second strategy was the Facebook platform, which encouraged developers to create products and services inside Facebook's walled

garden. The potent mix of newsfeed, platform, and a subset of bad actors leveraging both, combined to deliver us the Cambridge Analytica scandal. But, it is important to remember that Cambridge Analytica was a predictable outgrowth of the governance decisions taken, or not, by all parties, including government.

Facebook's business model is driven by its role as the largest data broker in the history of technology. To understand Facebook, we must understand the business model of online advertising. The technology infrastructure that allows companies like Facebook to identify exactly the right message to put in front of exactly the right person at exactly the right time is, in all aspects of the word, marvelous. But, the externalities of manufacturing and selling attention have not been fully examined.

The Cambridge Analytica scandal has finally focused our attention on these externalities, and we should use this opportunity to go beyond the specifics of that incident and consider broader implications. The failure of Facebook's platform initiative is not a failure of the concept of an open platform. It is, instead, the failure by an immature company to properly govern its platform, as well as the failure of society to govern the environment in which Facebook operates. Truly open platforms are regulated in a way that allows for economic and social prosperity for all. The wrong conclusion to draw from Cambridge Analytica's—is that it—entities like Facebook must build higher walls around their data. Our conclusion should be the opposite. A truly open society should allow individuals and properly governed third parties to securely share their data so as to create a society of what Nobel laureate Edmond Phelps calls "mass flourishing." The Cambridge Analytica scandal may seem to be entirely about a violation of privacy, but, to truly understand its impact, we must consider the implications to future economic innovation. Facebook has used the scandal as an excuse to limit third-party data-sharing across its platform. While this seems logical on first glance, it is, in fact, destructive to long-term economic value creation.

While I understand the lure of sweeping legislation that attempts to cure the ills of technological progress, such approaches often have their own unexpected consequence. The EU's adoption of GDPR, drafted to limit the power of companies like Facebook, may only strengthen that company's grip on its market while severely limiting entrepreneurial innovation. Instead, focused regulatory efforts to ensure secure and viable data portability, as well as a rethinking of core antitrust principles, are sorely needed.

Another mistaken belief to emerge from Cambridge Analytica is that any company, no matter how powerful or well-intentioned, can alone fix the problems the scandal has revealed. Facebook's impact on our society outstrips its ability to manage the externalities it has created. Fortunately, in recent months, Facebook has begun to reach out to the outside world with programs like the Election Commission and others that bring the outside in. These efforts should be encouraged.

We should strive to create a flexible, secure, and innovation-friendly approach to data governance that allows control by all affected parties, including the beneficiaries of future innovation. To play forward the current architecture of data in our society where

most of the valuable data is controlled by an oligarchy of massive corporations is to imagine a sterile landscape hostile to innovation. Most observers of technology agree that data is a new class of currency. The manufacturing of data into dollars is the main business of Facebook and many other large Information Age businesses. Currently, the only participatory right in this value creation for a user of these services is to either engage with them or purchase the stock of the company which offers the services. Neither of these options afford the user or our society compensation commensurate with the value created for the firm. We can, and must, do better for our society, and we can, and must, expect more of our business leaders.

Thank you very much.

[The prepared statement of Mr. Battelle follows:]

PREPARED STATEMENT OF JOHN BATTELLE, CHIEF EXECUTIVE OFFICER, NEWCO

Honorable Committee Members——

My name is John Battelle, for more than thirty years, I've made my career reporting, writing, and starting companies at the intersection of technology, society, and business. I appreciate the opportunity to submit this written and verbal testimony to your committee.

Over the years I've written extensively about the business models, strategies, and societal impact of technology companies, with a particular emphasis on the role of data, and the role of large, well-known firms. In the 1980s and 90s I focused on Apple and Microsoft, among others. In the late 90s I focused on the nascent Internet industry, the early 2000s brought my attention to Google, Amazon, and later, Twitter and Facebook. My writings tend to be observational, predictive, analytical, and opinionated.

Concurrently I've been an entrepreneur, founding or co-founding and leading half a dozen companies in the media and technology industries. All of these companies, which span magazines, digital publishing tools, events, and advertising technology platforms, have been active participants in what is broadly understood to be the "technology industry" in the United States and, on several occasions, abroad as well. Over the years these companies have employed thousands of staff members, including hundreds of journalists, and helped to support tens of thousands of independent creators across the Internet. I also serve on the boards of several companies, all of which are deeply involved in the technology and data industries.

In the past few years my work has focused on the role of the corporation in society, with a particular emphasis on the role technology plays in transforming that role. Given this focus, a natural subject of my work has been on companies that are the most visible exemplars of technology's impact on business and society. Of these, Facebook has been perhaps my most frequent subject in the past year or two.

Given the focus of this hearing, the remainder of my written testimony will focus on a number of observations related generally to Facebook, and specifically to the impact of the Cambridge Analytica story. For purposes of brevity, I will summarize many of my points here, and provide links to longer form writings that can be found on the open Internet.

Facebook broke through the traditional Valley startup company noise in the mid 2000s, a typical founder-driven success story backed by all the right venture capital, replete with a narrative of early intrigue between partners, an ambitious mission ("to make the world more open and connected"), a sky-high private valuation, and any number of controversial decisions around its relationship to its initial customers, the users of its service (later in its life, Facebook's core customers bifurcated to include advertisers). I was initially skeptical about the service, but when Sheryl Sandberg, a respected Google executive, moved to Facebook to run its advertising business, I became certain it would grow to be one of the most important companies in technology. I was convinced Facebook would challenge Google for supremacy in the hyper-growth world of personalized advertising. In those early days, I often made the point that while Google's early corporate culture sprang from the open, interconnected world wide web, Facebook was built on the precept of an insular walled garden, where a user's experience was entirely controlled by the Facebook service itself. This approach to creating a digital service not only threatened the core business model of Google (which was based on indexing and creating value

from open web pages), it also raised a significant question of what kind of public commons we wanted to inhabit as we migrated our attention and our social relationships to the web. (Examples: *https://battellemedia.com/archives/2012/02/its-not-whether-googles-threatened-its-asking-ourselves-what-commons-do-we-wish-for; https://battellemedia.com/archives/2012/03/why-hath-google-forsaken-us-a-meditation*)

In the past five or so years, of course, Facebook has come to dominate what is colloquially known as the public square—the metaphorical space where our society comes together to communicate with itself, to debate matters of public interest, and to privately and publicly converse on any number of topics. Since the dawn of the American republic, independent publishers (often referred to as the Fourth Estate—from pamphleteers to journalists to bloggers) have always been important actors in the center of this space. As a publisher myself, I became increasingly concerned that Facebook's appropriation of public discourse would imperil the viability of independent publishers. This of course has come to pass.

As is well understood by members of this committee, Facebook employed two crucial strategies to grow its service in its early days. The first was what is universally known as the News Feed, which mixed personal news from "friends" with public stories from independent publishers. The second strategy was the Facebook "Platform," which encouraged developers to create useful (and sometimes not so useful) products and services inside Facebook's walled garden service. During the rise of both News Feed and Platform, I repeatedly warned independent publishers to avoid committing themselves and their future viability to either News Feed or the Platform, as Facebook would likely change its policies in the future, leaving publishers without recourse. (Examples: *https://battellemedia.com/archives/2012/01/put-your-taproot-into-the-independent-web; https://battellemedia.com/archives/2012/11/facebook-is-now-making-its-own-weather; https://shift.newco.co/we-can-fix-this-f-cking-mess-bf6595ac6ccd; https://shift.newco.co/ads-blocking-and-tackling-18129db3c352*)

Of course, the potent mix of News Feed and a subset of independent publishers combined to deliver us the Cambridge Analytica scandal, and we are still grappling with the implications of this incident on our democracy. But it is important to remember that while the Cambridge Analytica breach seems unusual, it is in fact not—it represents business as usual for Facebook. Facebook's business model is driven by its role as a data broker. Early in its history, Facebook realized it could grow faster if it allowed third parties, often referred to as developers, to access its burgeoning trove of user data, then manipulate that data to create services on Facebook's platform that increased a Facebook user's engagement on the platform. Indeed, in his early years as CEO of Facebook, Mark Zuckerberg was enamored with the "platform business model," and hoped to emulate such icons as Bill Gates (who built the Windows platform) or Steve Jobs (who later built the iOS/app store platform).

However, Facebook's core business model of advertising, driven as it is by the brokerage of its users' personal information, stood in conflict with Zuckerberg's stated goal of creating a world-beating platform. By their nature, platforms are places where third parties can create value. They do so by leveraging the structure, assets, and distribution inherent to the platform. In the case of Windows, for example, developers capitalized on Microsoft's well-understood user interface, its core code base, and its massive adoption by hundreds of millions of computer users. Bill Gates famously defined a successful platform as one that creates more value for the ecosystem that gathers around it than for the platform itself. By this test—known as the Gates Line—Facebook's early platform fell far short. Developers who leveraged access to Facebook's core asset—its user data—failed to make enough advertising revenue to be viable, because Facebook (and its advertisers) would always preference Facebook's own advertising inventory over that of its developer partners. In retrospect, it's now commonly understood in the Valley that Facebook's platform efforts were a failure in terms of creating a true ecosystem of value, but a success in terms of driving ever more engagement through Facebook's service.

For an advertising-based business model, engagement trumps all other possible metrics. As it grew into one of the most successful public companies in the history of business, Facebook nimbly identified the most engaging portions of its developer ecosystem, incorporated those ideas into its core services, and became a ruthlessly efficient acquirer and manipulator of its users' engagement. It then processed that engagement into advertising opportunities, leveraging its extraordinary data assets in the process. Those advertising opportunities drew millions of advertisers large and small, and built the business whose impact we now struggle to understand.

To truly understand the impact of Facebook on our culture, we must first understand the business model it employs. Interested observers of Facebook will draw ill-informed conclusions about the company absent a deep comprehension of its core

driver—the business of personalized advertising. I have written extensively on this subject, but a core takeaway is this: The technology infrastructure that allows companies like Facebook to identify exactly the right message to put in front of exactly the right person at exactly the right time are, in all aspects of the word, marvelous. But the externalities of manufacturing attention and selling it to the highest bidder have not been fully examined by our society. (Examples: *https://shift.newco.co/its-the-advertising-model-stupid-b843cd7edbe9; https://shift.newco.co/its-the-advertising-model-stupid-b843cd7edbe9; https://shift.newco.co/lost-context-how-did-we-end-up-here-fd680c0cb6da; https://battellemedia.com/archives/2013/11/why-the-banner-ad-is-heroic-and-adtech-is-our-greatest-technology-artifact; https://shift.newco.co/do-big-advertisers-even-matter-to-the-platforms-9c8ccfe6d3dc*)

The Cambridge Analytica scandal has finally focused our attention on these externalities, and we should use this opportunity to go beyond the specifics of that incident, and consider the broader implications. The "failure" of Facebook's Platform initiative is not a failure of the concept of an open platform. It is instead a failure by an immature, blinkered company (Facebook) to properly *govern* its own platform, as well as a failure of our own regulatory oversight to govern the environment in which Facebook operates. Truly open platforms are regulated by the platform creator in a way that allows for explosive innovation (see the Gates Line) and shared value creation. (Examples: *https://shift.newco.co/its-not-the-platforms-that-need-regulation-2f55177a2297; https://shift.newco.co/memo-to-techs-titans-please-remember-what-it-was-like-to-be-small-d6668a8fa630*)

The absolutely wrong conclusion to draw from the Cambridge Analytica scandal is that entities like Facebook must build ever-higher walls around their services and their data. In fact, the conclusion should be the opposite. A truly open society should allow individuals and properly governed third parties to share their data so as to create a society of what Nobel laureate Edmond Phelps calls "mass flourishing." My own work now centers on how our society might shift what I call the "social architecture of data" from one where the control, processing and value exchange around data is managed entirely by massive, closed entities like Facebook, to one where individuals and their contracted agents manage that process themselves. (Examples: *https://shift.newco.co/are-we-dumb-terminals-86f1e1315a63; https://shift.newco.co/facebook-tear-down-this-wall-400385b7475d; https://shift.newco.co/how-facebook-google-amazon-and-their-peers-could-change-techs-awful-narrative-9a758516210a; https://shift.newco.co/on-facebook-a156710f2679; https://battellemedia.com/archives/2014/03/branded-data-preferences*)

Another mistaken belief to emerge from the Cambridge Analytica scandal is that any company, no matter how powerful, well intentioned, or intelligent, can by itself "fix" the problems the scandal has revealed. Facebook has grown to a size, scope, and impact on our society that outstrips its ability to manage the externalities it has created. To presume otherwise is to succumb to arrogance, ignorance, or worse. The bald truth is this: Not even Mark Zuckerberg understands how Facebook works, nor does he comprehend its impact on our society. (Examples: *https://shift.newco.co/we-allowed-this-to-happen-were-sorry-we-need-your-help-e26ed0bc87ac; https://shift.newco.co/i-apologize-d5c831ce0690; https://shift.newco.co/facebooks-data-trove-may-well-determine-trumps-fate-71047fd86921; https://shift.newco.co/its-time-to-ask-ourselves-how-tech-is-changing-our-kids-and-our-future-2ce1d0e59c3c*)

Another misconception: Facebook does not "sell" its data to any third parties. While Facebook may not sell copies of its data to these third parties, it certainly sells *leases* to that data, and this distinction bears significant scrutiny. The company may not wish to be understood as such, but it is most certainly the largest data broker in the history of the data industry.

Lastly, the Cambridge Analytica scandal may seem to be entirely about a violation of privacy, but to truly understand its impact, we must consider the implications relating to future economic innovation. Facebook has used the scandal as an excuse to limit third party data sharing across and outside its platform. While this seems logical on first glance, it is in fact destructive to long term economic value creation.

So what might be done about all of this? While I understand the lure of sweeping legislation that attempts to "cure" the ills of technological progress, such approaches often have their own unexpected consequences. For example, the EU's adoption of GDPR, drafted to limit the power of companies like Facebook, may in fact only strengthen that company's grip on its market, while severely limiting entrepreneurial innovation in the process (Example: *https://shift.newco.co/how-gdpr-kills-the-innovation-economy-844570b70a7a*)

As policy makers and informed citizens, we should strive to create a flexible, secure, and innovation friendly approach to data governance that allows for maximum innovation while also insuring maximum control over the data by all effected par-

ties, including individuals, and importantly, the beneficiaries of future innovation yet conceived and created. To play forward the current architecture of data in our society—where most of the valuable information is controlled by an increasingly small oligarchy of massive corporations—is to imagine a sterile landscape hostile to new ideas and mass flourishing.

Instead, we must explore a world governed by an enlightened regulatory framework that encourages data sharing, high standards of governance, and maximum value creation, with the individual at the center of that value exchange. As I recently wrote: "Imagine . . . you can download your own Facebook or Amazon "token," a magic data coin containing not only all the useful data and insights about you, but a control panel that allows you to set and revoke permissions around that data for any context. You might pass your Amazon token to Walmart, set its permissions to "view purchase history" and ask Walmart to determine how much money it might have saved you had you purchased those items on Walmart's service instead of Amazon. You might pass your Facebook token to Google, set the permissions to compare your social graph with others across Google's network, and then ask Google to show you search results based on your social relationships. You might pass your Google token to a startup that already has your genome and your health history, and ask it to munge the two in case your 20-year history 1of searching might infer some insights into your health outcomes. This might seem like a parlor game, but this is the kind of parlor game that could unleash an explosion of new use cases for data, new startups, new jobs, and new economic value."

It is our responsibility to examine our current body of legislation as it relates to how corporations such as Facebook impact the lives of consumers and the norms of our society overall. Much of the argument around this issue turns on the definition of "consumer harm" under current policy. Given that data is non-rivalrous and services such as Facebook are free of charge, it is often presumed there is no harm to consumers (or by extension, to society) in its use. This also applies to arguments about antitrust enforcement. I think our society will look back on this line of reasoning as deeply flawed once we evolve to an understanding of data as equal to—or possibly even more valuable than—monetary currency.

Most observers of technology agree that data is a new class of currency in society, yet we continue to struggle to understand its impact, and how best to govern it. The manufacturing of data into currency is the main business of Facebook and countless other information age businesses. Currently the only participatory right in this value creation for a user of these services is to A/engage with the services offered and B/purchase the stock of the company offering the services. Neither of these options affords the user—or society—compensation commensurate with the value created for the firm. We can and must do better as a society, and we can and must expect more of our business leaders.

(More: *https://shift.newco.co/its-time-for-platforms-to-come-clean-on-political-advertising-69311f582955; https://shift.newco.co/come-on-what-did-you-think-they-do-with-your-data-396fd855e7e1; https://shift.newco.co/tech-is-public-enemy-1-so-now-what-dee0c0cc40fe; https://shift.newco.co/why-is-amazons-go-not-bodega-2-0-6f14807 5afd5; https://shift.newco.co/predictions-2017-cfe0806bed84; https://shift.newco.co/ the-automatic-weapons-of-social-media-3ccce92553ad*)

Senator MORAN. Thank you very much.

Dr. Kogan.

STATEMENT OF DR. ALEKSANDR KOGAN, LECTURER, DEPARTMENT OF PSYCHOLOGY, UNIVERSITY OF CAMBRIDGE

Dr. KOGAN. Thank you, Chair and Senators, for inviting me to speak to you today.

The last few months have been both extremely difficult and eye-opening. As I've watched what has unfolded, I've naturally taken a hard look in the mirror at my own role in the controversy. What is clear to me now is that I made a mistake in not appreciating how people would feel about us using their data. And for that, I'm deeply sorry.

We thought collecting people's data like we did was completely normal, accepted, and that people whose data was being collected and transferred knew that it was regularly happening. This seem-

ing normalcy and regularity of data transfer among developers and tech companies, in my view, is perhaps what is most concerning about the whole situation, because it means that people and companies have done, and will do, projects where data will be moved and used in ways consumers don't fully appreciate. And, indeed, that's what we have in the tech, a largely unregulated massive industry with many people working in ways that we now have to seriously wonder if the general public is OK with or even knows about. The industry doesn't have the same reputation for skulduggery as finance has had over the recent financial crisis. But, the culture of "ask for forgiveness and not permission," in my view, is just as present in tech as it is in finance.

As I've reflected on what the public is concerned about, I see two core possibilities. First, people may feel angry and violated if they think their data may have been used as part of a mind-control effort, that somehow Cambridge Analytica had figured out their inner demons, weaponized the Internet, and used this ability to dupe them into voting in a particular way, when otherwise they would not have. This is science fiction. The data is entirely ineffective for micro-targeting. And, in fact, I believe psychographics, as a whole, is a dead-end for this purpose. There is value to the data if you're trying to understand the general trends over big groups of people, but, for any one person, it simply doesn't work. As an academic psychologist, I thought it might work, but, as I discovered, psychographics was an experiment that failed.

The second possibility of what is troublesome to people is, regardless of the data's efficacy, people may still feel angry and violated by the fact that their data could have been, and was, accessed by others. Just the very fact that data can be accessed elicits a strong visceral response. And we know from research in psychology that it is our emotions that drive our moral judgments. And emotions such as anger, disgust, and violation gives us a window into what we judge to be moral and immoral. I think this emotional reaction is entirely understandable and begs the question of, How do we tackle the broad issue of data privacy? It's a big problem, and one that the current controversy is finally bringing into focus for the public.

In thinking about how we solve the problem, I keep coming back to the tension between the financial incentives of ad-dependent tech companies and our American values of autonomy and free choice. Any solution, in my view, needs to be respectful of people's right to choose. Critically, however, our ability to choose wisely begins with understanding. People need to know and appreciate both the benefits and dangers of sharing their data with the Facebooks and Googles of the world.

The current way tech companies get at people's concerns, I think, is fundamentally broken. It encourages people not to read, not to be informed, and doesn't outline the real, specific scope of how the data will be used. If we could find a way to get companies to act fairly toward consumers, asking for truly informed consent, and getting granular with the consumers about how their data will be used, I believe this will go a long way in tackling these issues.

I think there are challenges to tech companies doing this themselves. They are under enormous financial pressure to gobble up

more and more of our data so they can deliver better and better personalized ads. And the dirty secret in the industry is that these ads right now are just not that effective—not useless, but not as effective as we'd want. So, companies want more, and not less, data so they can do better. And so, data becomes the most valuable currency.

Under these conditions, opt-in consent could be an existential threat. It risks companies losing much of the treasure trove they have worked so hard to build. I don't know the proper framework for a solution. That is not my expertise. But, these are the tensions I've been thinking about around the problem.

I look forward to answering your questions today and hearing from my co-panelists about their perspectives on this critical topic.

Thank you, again, for the opportunity to be here and speak with you today.

[The prepared statement of Dr. Kogan follows:]

PREPARED STATEMENT OF DR. ALEKSANDR KOGAN, LECTURER, DEPARTMENT OF PSYCHOLOGY, UNIVERSITY OF CAMBRIDGE

Chair and Members of the Subcommittee:

The past several months have seen a myriad of allegations and claims made about myself, Cambridge Analytica, and Facebook in relation to a project carried out in the summer of 2014. Some of this information has been accurate, while other aspects have been speculation, exaggeration, or misinformation. My hope is to help the Subcommittee understand what is and is not legitimate from the various narratives that have emerged. I also wish to give my current thinking as to the important broader issues raised by the controversy surrounding Facebook and the privacy of user information.

My Background

I am a social psychologist whose academic work focuses on well-being, kindness, and compassion. To study these topics, my lab and I have used a variety of methods, including surveys, behavioral studies, and social media. I received my B.A. degree in Psychology from the University of California, Berkeley, in 2008 and a Ph.D. in Psychology from the University of Hong Kong in 2011. Since 2012, I have been a Research Associate and University Lecturer at the University of Cambridge (the "University") in the Department of Psychology. At the University, I have conducted research, taught classes, and supervised graduate and undergraduate research work through the Cambridge Prosociality and Well-being Laboratory (the "CPW Lab")—which I founded. All of my academic work was reviewed and approved by the University's ethics committees.

My Collaboration with Facebook and the CPW Lab App

In early 2013, I began collaborating with Facebook on studies aimed to understand how people around the world connect and express emotions. Throughout 2013, Facebook provided me with several macro-level datasets on friendship connections and emoticon usage. These were aggregated datasets, typically at the country level (*e.g.,* number of friendship connections between USA and UK), which did not contain specific information about individual Facebook users. Using this data, members of my lab began writing papers together with Facebook personnel.

During this active collaboration with Facebook, I created a Facebook app, which I called the CPW Lab App (after the name of my lab), in order for us to collect individual Facebook users' data to pair with the aggregated data Facebook had provided directly. For studies based on data derived from the app, we asked participants to complete a survey and provide information from their Facebook accounts by logging in through the Facebook application portal. The terms of service of the CPW Lab App were contained in a link on the Facebook application portal's login page. The terms of service indicated that the data would be used for academic purposes. Data derived from the CPW Lab App was not provided to SCL.

The GSR App and Data Collection

I was introduced to SCL through a Ph.D. student at the University in winter of 2014. He introduced me to Chris Wylie, who represented SCL at the time. Our con-

versations began with Mr. Wylie detailing his experiences working for the Obama campaign. He asked me to provide survey-consulting services to SCL, including collecting data from Facebook and generating personality profiles.

To do the project, a fellow University research psychologist and I registered a company, Global Science Research ("GSR"), in the UK. Mr. Wylie held himself out to us as a data law expert, having studied law at a London university, and he served as our guide on how to be compliant with legal requirements and prohibitions.

Before we started collecting data from survey participants, GSR changed the name and terms of service of the CPW Lab App. The terms of service were provided to us by Mr. Wylie. References to academic use and the University were deleted from the terms of service, and the name of the application was changed from "CPW Lab App" to "GSR App." GSR also changed the terms of service of the application to reflect the expected use of the data. When individuals who participated in the survey logged into Facebook through the GSR App portal, Facebook presented a link to the GSR App's terms of service, which informed each participant as follows:

> [i]f you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data . . . and grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data and contribution for any purpose.

The terms of service also informed each survey participant that GSR would collect "any information that [the participant] choose[s] to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network."

After the participants entered their Facebook credentials into the GSR App Facebook login portal, they were taken back to the third-party survey vendor's website to complete the survey. GSR collected data from the survey participants and their friends whose Facebook privacy settings were set to allow the participants access to their information. The data collected from participants and friends included, if available, an individual's name, birth date, location (city and state), gender and the Facebook pages each user had "liked." As with the CPW Lab iteration of the application, information was collected from friends whose Facebook privacy settings were set to provide the survey participants access to the friends' "likes" and demographic information.

In the end, approximately 30 million personality profiles based on this information, plus a limited amount of demographic data and certain "likes," were transferred to SCL.

In the latter part of 2014, after the GSR App data collection was complete, GSR revised the application to become an interactive personality "quiz" called "thisisyourdigitallife." The commercial portions of the terms of service that had been added to the GSR App were not changed. The thisisyourdigitallife App was used by only a few hundred individuals and, like the two prior iterations of the application, collected demographic information and data about "likes" for survey participants and their friends whose Facebook privacy settings gave participants access to "likes" and demographic information. Data collected by the thisisyourdigitallife App was not transferred to SCL.

Micro-targeting on Facebook

A point of confusion has been whether the data we collected would be useful for micro-targeting ads on Facebook. I believe the project we did had little to no use for someone wanting to run targeted ads on Facebook. The Facebook ads platform already provided SCL with many tools to run targeted ads with little need for our work—in fact, to this day, the platform's tools provide companies a far more effective pathway to target people based on their personalities than using personality profiles for Facebook users developed by myself and my fellow social psychologists.

Negative Public Reaction

In reflecting on the SCL project and the public reaction from media reports, I perceive two primary reasons for public concern. First, people may feel angry and violated to the extent that their data may have been used as part of a mind-control effort; that somehow SCL had figured out their inner demons, weaponized the internet, and used this ability to dupe them into voting a particular way when otherwise they would not have. This concern rests on an incorrect premise about the data and its utility. I believe there is almost no chance this data could have been helpful to a political campaign—and I still have not seen any evidence to indicate that the

Trump campaign used this dataset to micro-target voters. The arguments for its utility fall apart under legitimate scientific scrutiny, and I would be happy to talk in greater detail about the underlying issues.

Second, regardless of the data's efficacy, people may feel angry and violated to the extent that their data could have been and was accessed by others without their appreciating the actual access they were giving third parties. This is an understandable emotional reaction upon realizing how much data was being conveyed directly and indirectly. I'm very regretful that I did not better anticipate this reaction. If the heart of the controversy lies in this second issue, I believe it points to a much broader problem with how companies interact with consumers in the tech space—in particular, the conduct of companies whose business model is predicated on digital advertising.

Roots of the Controversy

Given what we now know, I believe that a situation like the present one was inevitable. For decades, a shift occurred in how consumers interacted with companies. The interaction used to be quite simple: Company gives us product, we give company money. It was typically impersonal and arms-length. Then digital marketing came into existence, and new companies arose with a new formula: They give us technological products and services, not in exchange for money, but in exchange for intimate details about ourselves that we are willing to share. It is our photos, thoughts, emotions, and connections. These things become valuable to companies, and they use this information to monetize us to their actual clients: Advertisers. We became the product. This new relationship between company and consumer is extremely complicated and personal. But the primary vehicle we have had to manage this relationship has been a "terms of service" document that is often unhelpful to the average consumer.

A core aspect of many of these documents is the idea of blanket consent: The consumer gives broad rights for a company to do whatever it likes with the data. For instance, here is an excerpt from the Facebook Terms of Service from 2014 (section 2.1):

> For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License).

Blanket consent such as this is standard industry practice—Facebook is hardly alone in using language like this. It was and still is normal for companies to ask consumers to grant them broad rights to do whatever the companies like with the data. The widespread use of such agreements, in my view, created a near certainty that at some point consumers would be unpleasantly surprised by the specific way a company used their data. Consumers may have technically agreed to broad usage, but nonetheless the feelings of outrage and being wronged that have been released by the Cambridge Analytica controversy are the inevitable response.

Tackling the Issue

Trying to fix this problem will not be simple. My expertise provides one perspective on the issues—and so I very much look forward to a dialogue with others to contribute to public awareness and broaden my own understanding of the various forces at play.

As a general matter, businesses are typically able to respond to consumer needs and dissatisfaction, but this may be difficult for those businesses that have a strong financial incentive to collect more and more data. Companies whose main revenue comes from ads are typically selling advertisers on the idea that the companies can find the right person, in the right place, at the right time, and serve them the right ad. This may act as a barrier to change.

In fact, digital ads, in particular on social media, are far less effective than one might think. For example, in the only paper I know of to have tested the idea of tailoring Facebook ads based on people's personalities, the researchers found that less than 1 in 100 actually clicked the ad. And of those few people, fewer than five in 100 did what the ad wanted them to do—buy a product. Facebook and companies like it are under enormous pressure to do better. That often means they want more and more data about us to build better and better models. Enhancing consumer consent, such as requiring opt-in consent, jeopardizes their ability to collect more and more data—in fact, opt-in consent will likely strip away much of the data the companies have today. So I believe companies are likely to strongly resist making

changes themselves for fear that others will not follow suit and they will be at a competitive disadvantage.

A second important issue is the role of autonomy and individual responsibility. We as Americans strongly cherish our ability to choose—we see it in our system of government and in our approaches to consumer goods. So I believe any solution needs to be respectful of people's right to choose. Critically, however, this ability to choose must be predicated on being informed about (a) what a person is consenting to and (b) the risks of giving consent. In short, people must give true informed consent. However, the kinds of blanket approaches to consent used by major data-monetizing companies like Facebook run counter to true informed consent.

Some Possible Responses

In my view, thinking through the means of achieving informed consent is the key to avoiding a future Cambridge Analytica situation. I see a few ways we can start going down this road. First, I would suggest we find ways to give consumers the information they need about how their data will be used—and these planned uses need to be specific rather than abstract and general. Rather than a broad license, companies could outline specifically how the data will be used (*e.g.,* for advertising about consumer products, advertising about political campaigns, building models of your values and preferences). This will avoid consumers being caught off guard later on.

Second, consumers may need some kind of risk assessment of what could go wrong—companies should be upfront about what dangers exist in placing data on their platform and what they are doing to protect against those risks.

Third, we should consider requiring that consumers give opt-in consent. It should not be taken as a given that a person agrees with everything unless they say they disagree; it is important for people to make an affirmative act of agreement to demonstrate the making of a decision.

Fourth, we could consider requiring consent to be given to each specific point in the consent document rather than globally. This would give consumers the ability to choose what they are and are not comfortable with, and also incentivize companies to provide shorter, more readable documents.

Fifth, we should look for ways to prevent or at least discourage consent being given without consumers reading—or even seeing—the disclosures. Facebook currently allows consumers and developers alike to sign up to their main service and their apps without being required to see the terms of service. They are hard to find, easy to miss, and do not always require an affirmative manifestation of consent. This, in my view, runs counter to the notion of true informed consent from consumers.

Conclusion

In sum, my view is that we should think hard about finding ways to empower consumers, giving them the ability to make more informed decisions about how their data is used. This, I fear, cannot be left entirely to companies and consumers to work out among themselves as business interests may run counter to consumer privacy interests because of present revenue models.

Senator MORAN. Thank you very much.

Mr. Soltani.

STATEMENT OF ASHKAN SOLTANI, SOLTANI LLC, AND FORMER CHIEF TECHNOLOGIST, FEDERAL TRADE COMMISSION

Mr. SOLTANI. Chairman Moran, Ranking Member Blumenthal, and distinguished Members of this Subcommittee, thank you for the opportunity to testify today.

I'd like to present a few opening remarks, but would be happy to submit the rest of my testimony for the record.

I actually had the honor of addressing this very Committee in 2011 to describe the state of online privacy. During that hearing, I outlined the pervasiveness of online tracking, how notice and choice is ineffective, and the needs for intervention. Today, some 7 years later, nearly all of what I said still applies, although now with much greater urgency. While policy has changed very little

during that time, the companies' abilities to invade and exploit individuals' information has grown tremendously.

I have researched and written about online privacy for the greater part of the last decade, and I have three points to make today. One, this problem is not novel or new. It's actually the underlying business model for Facebook and much of the Internet at large: growth at any cost. Two, our consumer protection framework is broken. Specifically, notice and choice in a monopolistic market where there is no market choice is insufficient to protect consumers. And three, the privacy invasion from online tracking is wildly intrusive, and yet we provide consumers very little protection.

Senators, all of this has happened before, and all of it will happen again. I cannot stress enough, Cambridge Analytica's access and sale of personal information from Facebook is not new. It's a foreseeable result of a business model that essentially pays developers with access to consumer information. Essentially, to maintain its dominant position in the market, Facebook needs to grow on as many devices and partner with as many websites as possible. And, rather than build each app or initiate a partnership with each website, Facebook incentivizes its partners to develop apps or integrate with its social widgets, providing these third parties with in-kind compensation, compensation in the form of robust information about consumers' identities, activities, likes, and preferences. This includes information not just about the users themselves, but also about their friends. In the case of device makers recently covered in the *New York Times,* this access was provided even when users attempted to block third-party access via Facebook's privacy—platform privacy controls.

Second, the current framework of notice and choice is inadequate. Our entire U.S. policy framework around privacy is built upon notice and choice. A company discloses to a consumer information about its practices, and users consent to those practices by using the company's site or website—site or service. The FTC's privacy enforcement authority is predicated on this, as are many of our State laws. However, in practice, this framework does nothing to protect consumers. It's well understood that users neither read nor understand most companies' privacy policies. Mr. Zuckerberg, himself, testifying earlier this year in front of a joint committee hearing, admitted that he did not expect users to read lengthy, verbose privacy policies.

What's more, even if users did actually read the privacy policies, they have no way, short of boycotting the service, to object to the privacy practices they find intrusive. Indeed, ignoring for a moment the dominance of Facebook as a destination website or mobile app, it's also the primary method by which users log on to third-party services, like dating apps, social websites, et cetera. Today, Facebook serves as the de facto single-sign-on identity provider for the Internet. If you want to use Tinder, Bumble, SoFi, or if you want to verify yourself as a host on Airbnb, you need to have a Facebook profile. So, Senators, consumers consent to what they do not read or understand, nor is it practical for them to do otherwise.

And last, Senators, the privacy harms at issue are incredibly invasive. While friends argue that this information is not sen-

sitive—photos of our cats or Happy Birthday and Father's Day updates—users feel quite the opposite. Time and time again, we see stories emerge from individuals who are convinced that Facebook eavesdropped on them through their smartphone's microphone in order to target ads. In consumers' eyes, Facebook's targeting is to intimate, so intrusive that it could only be the result of a company monitoring their private conversations. While I and other researchers have found very little evidence to support claims of Facebook's accessing microphone without permission, the claims themselves shed light into how invasive behavioral inferences can be. Essentially, inferences made from monitoring our activities online are equivalent, if not greater, than what may be possible from eavesdropping on our private conversations. Yet, our currency—our current privacy framework provides little or no protection for our online behavioral data, certainly not the affirmative consent necessary for recording conversations or collecting our location.

These problems will simply not vanish. Companies we're discussing today will not simply abandon their practices without reason. Facebook's business models of leveraging consumer data for market growth fundamentally puts consumers at risk. "Growth at any cost" is the new "unsafe at any speed." It's far past time for Congress to bring its considerable resources to bear on this effort.

I really look forward to your questions, as well.

Thank you.

[The prepared statement of Mr. Soltani follows:]

PREPARED STATEMENT OF ASHKAN SOLTANI,[1] INDEPENDENT PRIVACY RESEARCHER AND CONSULTANT

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' behav-

[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.commerc e.senate.gov/public/_cache/files/f4645a61-b16e-4fa7-a18c-f0361268f356/F94C2CFDD06D91AE3A9E044F9D888E6E.soltani-testimony.pdf.*

iors, the government has remained static, and has not brought its considerable resources to bear on this issue.

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 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.

---

[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.*

[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.*

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 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.

---

[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.*

[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-identifia ble-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.

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 ex-

---

[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.*

[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.*

plains, 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 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 Cali-

---

[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.*

fornia 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.

Senator MORAN. Thank you very much.

We'll now have a round of questions and answers.

And I'll begin with Dr. Kogan. Would you describe the individual Facebook user data that Cambridge Analytica gained access to through the personality-test app that you designed?

Dr. KOGAN. Yes, Senator.

So, we provided them approximately 30 million people's worth of data. This dataset had people's name, it had their location, it had their birth dates, their gender, and then it listed a number of predictive personality traits, things like extroversion, agreeableness, and openness to experience. We also provided a very limited number of specific page Likes. This number the—Cambridge Analytica chose about 500 page Likes from a list of about 150 million. And so, we checked. And so, it was a small percentage of the total page Likes.

Senator MORAN. Your testimony and past statements clearly indicate that you question the effectiveness of the Facebook user data to micro-target voters in political campaigns. Would you provide additional details of the legitimate scientific scrutiny described in your testimony regarding the effectiveness of using this data?

Dr. KOGAN. Absolutely.

So, to be honest, going in, I thought it would be a lot more effective. Part of the issue is, most psychologists, when we do research, we're not really studying the specific person, we're not studying Senator Moran, we're studying people in general. With this project, we had to really think about how accurate we are, and we found we're just not. So, for example, there are five personality traits we're trying to predict. We found that, for only about 1 percent of the users were we accurate about all five traits. For 6 percent, we were wrong about everything. And, in fact, when we dug further, we found that our accuracy wasn't really much better than simply assuming everybody is average in everything.

There are many other ways to tackle this issue. It gets a little technical and scientific. But, that's just the flavor for how we realized it's just not quite effective.

Senator MORAN. How were you able to determine the ineffectiveness? How were you able to make the comparison?

Dr. KOGAN. So, normally what we do is, we collect a large number of people. And here we had over 200,000 people. And we build a model on a subset of them. Say, we take 100,000, we put them aside, and we build a model. But, then we have the other 100,000 for whom we could both predict the data and we have their true responses. We actually have their survey responses to the personality test. And that's what we do. We build a model on one half,

---

[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).

then predict it for the other half, and compare it to their real answers. And there, we could actually check it.

Senator MORAN. Your testimony indicates that Facebook's tools provide companies a far more effective pathway to target people based upon their personalities than the profile you developed in your project. Describe those tools and their effectiveness.

Dr. KOGAN. Yes, Senator.

So, in short, if the goal of Cambridge Analytica was to show personalized ads on Facebook based on people's personalities, what they did was stupid. What you actually—because here's why it doesn't make sense. It's 30 million people. Facebook has over 200 million people in the United States. And the models are based purely on people's page Likes, which is a pretty rare behavior. Facebook gives you tools where you could target 100 percent of the user base and use a lot more of the data. And the way you would do this is use their advertising platform, the lookalike audience. And what you could just supply to Facebook is a list of e-mail addresses, which you can get from a survey, where people fill out a personality test plus give you their e-mail address. And you could choose the 20 percent that are the most extroverted, take those e-mail addresses, go on Facebook and say, "Please find me people like this." And Facebook will use a lot more of its data than just the page Likes to try to build models and find the rest of the extroverts. So, this would be more effective, and you would reach not only the 15 percent that we had, but the 100 percent. It would still be largely ineffective, but it would be a step in the right direction.

Senator MORAN. Mr. Battelle, you reacted to some of the things that Dr. Kogan said as I watched you.

Mr. BATTELLE. I didn't realize that my testimony included, you know, mute responses.

[Laughter.]

Senator MORAN. I was going to give you the opportunity to verbalize those——

[Laughter.]

Senator MORAN. What did you—what should we take from Dr. Kogan's comments just now?

Mr. BATTELLE. I think, while, you know, many of the comments that Dr. Kogan made about how we, as consumers of Facebook, feel about the data being used, which are—you know, we feel violated, and we're certain that more is being used—more is being known about us or listened to or surveilled. The truth is, is that the entirety of Facebook's data model, its ability to know about not only you as a person, but also as a potential cohort, what's known as a segment in Facebook, is extraordinarily powerful, far more powerful than, I think, anything that SCL or Cambridge Analytica might have done through this app.

Senator MORAN. Thank you.

Senator Blumenthal.

Senator BLUMENTHAL. There's no question that Facebook's model is immensely powerful and unchecked right now. And so, the challenge for us is to provide some oversight and protection, but, at the same time, prevent the inhibition of innovation and freedom. And so, I want to begin, Mr. Kogan, by exploring your points about terms of service. In fact, in our last hearing with Mr. Zuckerberg,

I held up the terms of service that I believe were provided to Cambridge Analytica by you, or by you to Cambridge Analytica. Do you recall that moment?

Dr. KOGAN. Yes, sir. Cambridge Analytica provided those terms of service to me to put in the app.

Senator BLUMENTHAL. Do you know the origins of those terms of service?

Dr. KOGAN. Chris Wylie wrote them. My understanding was that this would be a way for us to make a fully commercial app. Because, prior to that, it was an academic app.

Senator BLUMENTHAL. And those terms of service provided for the sale or sharing of information, did they not?

Dr. KOGAN. Yes, they did.

Senator BLUMENTHAL. And they were known to Facebook, were they not?

Dr. KOGAN. Yes, they were.

Senator BLUMENTHAL. Despite Mark Zuckerberg disclaiming any knowledge of them.

Dr. KOGAN. I don't know if he personally knew about it, but we certainly provided the terms to Facebook.

Senator BLUMENTHAL. There's no question that Facebook knew about those terms of service.

Dr. KOGAN. At the very least, they had them and could have taken a look.

Senator BLUMENTHAL. Mr. Battelle, Facebook, for years, was the best friend that data brokers could have. In March, Facebook announced that it was shutting down the data broker program to, "help improve people's privacy on Facebook." According to public reports, Facebook initially told ad agencies they'd be prohibited from uploading lists of potential prospects acquired from data brokers. Two days later, advertisers' complaints persuaded Facebook to allow them to continue targeting Facebook users with ads based on uploaded customer lists purchased from those data brokers.

You, sir, are on the Board of Acxiom, one of Facebook's primary partners in that arrangement. And it has had extensive involvements with the online advertising market. I mention those facts just in the interests of full disclosure. Did Facebook tell advertisers, in March, that they would not be allowed to use prospective customer lists acquired from data brokers? And is it true that they reversed that decision under pressure from the advertisers?

Mr. BATTELLE. I was not involved in those specific conversations, but that's my understanding, Senator. I think it's important to realize that the use of third-party information to target cohorts—not individuals, but cohorts, people with certain household income or people who live in certain regions—certainly predates the Internet. And this kind of information has been used to drive everything from——

Senator BLUMENTHAL. There's no question that advertisers target certain groups——

Mr. BATTELLE. Yes.

Senator BLUMENTHAL.—based on instinct and——

Mr. BATTELLE. There is a question as to whether or not instinct is not, in fact, better than the current data that we have to target. But, that's another hearing.

Senator BLUMENTHAL. Well, I think the difference may be that the data is based on what consumers submit.

Mr. BATTELLE. Yes.

Senator BLUMENTHAL. The instincts and gut feelings are based on what the PR guy may know or feel from his——

Mr. BATTELLE. Indeed.

Senator BLUMENTHAL.—or her perceptions. So, I think you've all very correctly stated that, for Facebook, consumers are the product, so to speak. Their information is monetized. They may feel they are, in fact, the customer, but it's the advertisers who are the customer.

Mr. BATTELLE. Right. And I'd like—to answer to your question, there was a—I don't know if Facebook would call it a reversal or, rather, a clarification—their major customers, the advertisers, need to know who their prospects are and bring in information about those prospects from their own databases, including information enriched from third parties, known as data brokers. And this is very standard, not only at Facebook, but at Google and almost every other online advertising platform. So, I think Facebook realized they had overstepped.

Senator BLUMENTHAL. And I think your characterization is correct, that they overstepped. It's one of the ways they've overstepped. And what we need to understand, as one of you said, consumer information is the new class of currency. In effect, we are the currency—you and I and everyone in this room, and everyone who is involved here.

I have other questions, Mr. Chairman, but, in deference to my colleagues, I'm going to yield to them. And we'll perhaps have a second round, if that's possible.

Senator MORAN. Senator Fischer.

Senator BLUMENTHAL. Otherwise, I'll go over my time.

Senator MORAN. Senator Fischer.

STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Mr. Chairman.

Mr. Battelle, you spoke of a concept that consumers online should be able to access all of their data for use in a flexible manner, via a token. And this reminded me that, in its response to my written hearing questions that I had sent to Facebook, they confirmed that, "much, but not all," of a user's data is contained in the file that it lets you download. I'd be interested in hearing your thoughts on user control. For example, should Facebook users be able to access a complete set of their respective personal data containing all information the company knows about them?

Mr. BATTELLE. Thank you, Senator.

My answer to that question is, "Absolutely." There is a very big difference between getting a CD-ROM file or a stack of paper or even a digital file that is not machine readable, that contains prohibitions on its aggregation and use by other third parties, and a token, which can be freely passed to any third party, with permissions that you can set, as the individual, to create more value. What I was suggesting in my written testimony is that an economy where we can, in fact, take these kinds of tokens, whether they are

from the large companies like Amazon or Facebook, or whether they're from small companies, and freely set revokable permissions, such that we can create new kinds of value by combining that data—I believe that an economy that has that kind of free flow of information and security and control, that is based on the individual, will be a society that is far greater in innovation than the one we have currently today.

Senator FISCHER. Can a Facebook user, right now, view how they're targeted with the ad targeting, with predictive analysis? Can they see that? Can I see how I'm viewed, what cohort I'm put in? Can I change that? Can I determine what cohort I want to be in?

Mr. BATTELLE. Not exactly, no. You can, with a new tool that has been announced, as I understand it, but has not yet been rolled out, called Ad Transparency. And I'm looking at the expert to the left, here. That will be the case, partially. However, that control piece is very limited, at this point. I do not think it should be, but it is.

Senator FISCHER. Mr. Soltani, do you have anything to add to that? Are you the expert that we were looking at?

Mr. SOLTANI. Possibly.

There are a set of tools. One is your interest manager that many of the advertisers provide. And those are, essentially, the categories of—or inferences—like you might be interested in buying a house, buying a car, you might be of a certain age—that you can control. There's also a new tool that they provided, which is to show you what marketers uploaded you as a audience list. Right? So, what—as was described earlier, what marketers upload your e-mail list to target you—or upload you in their e-mail list to target you. So, we do have those two tools. But, it's showing not the entirety of the data that's available to Facebook about your behaviors, both—it's mostly the data that you volunteered to the service.

Senator FISCHER. So, Facebook now is saying that—or they're putting forth a concept that users are in complete control of their data. Is that true? Are these new tools going to let Facebook users be in complete control?

Mr. SOLTANI. I think what they're—what the more accurate term would be—the new tools allow users to export a subset of the data, such as the photos and comments and status updates that they've given to the site. They don't get to see all of the inferences, all of the underlying data, all of the visits across the Web or the——

Senator FISCHER. So, I still won't know how I'm tagged?

Mr. SOLTANI. Not completely, no. I think another interesting point to add is, in—if we look back to 2011—I think it was 2011, Facebook versus Power Ventures was a case where another company had provided a tool to allow users to essentially pull their information off of Facebook and use it across a suite of services. It was, essentially, a data portability and data aggregation tool. Facebook sued the company and claimed copyright over consumers' information. So, they, when it protects their business interests, have actively thwarted other companies from accessing that data, but then, when they control the API and have benefits from those partnerships, will allow access. So, it's kind of an interesting piece around consumer control.

Senator FISCHER. Thank you.
Thank you, Mr. Chairman.
Senator MORAN. You're welcome.
Senator Markey.

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman. Thank you for this excellent hearing.

Mr. Soltani, as a former Chief Technologist at the Federal Trade Commission, do you believe that Facebook violated its 2011 consent decree with the Federal Trade Commission during this Cambridge Analytica debacle by sharing users' friends' information, overriding users' privacy preferences?

Mr. SOLTANI. Thanks, Senator Markey.

So, I, of course, have to preface this by saying all the opinions here are my own, in my personal capacity, and not of the FTC or any previous employer.

What I can say is, I—the facts around the, kind of, Cambridge Analytica sharing was quite similar to the facts in 2011 that were at hand. Right? So, the FTC complaint alleged that Facebook first—forced certain private information, such as friend lists, to be made public, when they were previously private, told users they could restrict data sharing to limited audience—for example, Friends Only—when, in fact, selecting Friends Only did not prevent information from being shared with third-party applications that their friends used, and that Facebook had a verified apps program that claimed it certified the security of participating apps, which it didn't. Right? So, those were the—kind of, the counts in the complaint. And the settlement in the consent decree said—it basically barred Facebook from making misrepresentations about the privacy security of consumers' personal information, and required Facebook to obtain consumers' affirmative express consent before enacting changes to override their privacy policy preferences.

I think the facts of the—both with Cambridge Analytica and the device partnerships showed that there were still instances where your privacy controls or information about you—for example, your—me being a friend of yours on Facebook—would be shared with apps, even though the representations were otherwise.

Senator MARKEY. Right. So——

Mr. SOLTANI. So, yes.

Senator MARKEY.—it—that would be a violation of the——

Mr. SOLTANI. I would say yes.

Senator MARKEY.—consent decree——

Mr. SOLTANI. Yes.

Senator MARKEY.—if that information was being shared. So, outside of the Cambridge Analytica episode, did Facebook violate the 2011 consent decree when it gave data access to 60 partner device makers, including Microsoft, Google, and BlackBerry, even when many users believed that they barred this sharing, as reported in the *New York Times* earlier this month?

Mr. SOLTANI. Again, in my personal opinion, I believe they did, particularly, as I have described in my testimony, that privacy set-

tings such as platform preferences could be overridden by certain device partners.

Senator MARKEY. So, in light of those revelations, should the Federal Trade Commission impose penalties on Facebook for violating the consent decree which Facebook reached with the Federal Trade Commission?

Mr. SOLTANI. Again, I believe the FTC has publicly said that they're investigating Facebook. And, you know, if I had to wager, I guess I would say—you know, it—I'm not a lawyer, so I can't specify to the—exactly how they will interpret the case, but I feel like there's a strong likelihood that—of imposing fines——

Senator MARKEY. I'm not asking you how——

Mr. SOLTANI. Yes.

Senator MARKEY.—you think they're going to condone?

Mr. SOLTANI. Yes.

Senator MARKEY. I'm asking how you would condone——

Mr. SOLTANI. I think they should. One——

Senator MARKEY. OK, that's important.

Mr. SOLTANI.—one of the challenges, though, is that, if you look—so, Facebook is a $40 billion company, in terms of annual revenue. The FTC's privacy settlements, their largest were either $22.5 million, for Google Safari, or $100 million, for LifeLock, which include advertising. I think even penalties on that order or more will do very little to actually——

Senator MARKEY. No, I agree with you. In order for this to be meaningful, the number has to be substantial. Otherwise, it's just paying a parking ticket——

Mr. SOLTANI. Exactly.

Senator MARKEY.—and then they move on, without even noticing it in their bottom line.

So, Mr. Soltani, do you have concerns about the fact that Facebook shared user data with devices made by Huawei, a Chinese company flagged by the intelligence community as a threat to national security? Do you believe that Facebook can say definitively that Facebook user data was never stored on Huawei servers?

Mr. SOLTANI. I think that's an important point, Senator. The issue at hand is that, by providing certain partners privileged access to user data, those partners effectively got to override user privacy settings. It's like having administrative access, in some ways, on—to Facebook data. And my understanding is that, once that data is off and transferred to those partners' handsets, it can be used in whatever way those partners see fit.

And, again, to cite an—a recent FTC case, the FTC brought an investigation—a settlement with a company called Blu, which was a Amazon seller, B-l-u, that was reselling handsets by Chinese manufacturers. Those handsets were found to be sending the complete contents of text messages and contents of the phone to the China's—the company's server in China. Right? So, were Blu to be one of those partners, or were Huawei to implement some of the same features, I don't think Facebook would have known or have had a way to monitor for that.

Senator MARKEY. Right. And so, you have the compromise of privacy of Americans and their information then becoming a national security issue, as well, because——

Mr. SOLTANI. That's right.

Senator MARKEY.—this company is on an American national security watch list. So, it just gets much more serious and, of course, concerning, which is why I'm so glad that we are having this hearing, Mr. Chairman. I yield back.

Senator MORAN. Thank you, Senator. You have nothing to yield back, but thank you.

[Laughter.]

Senator MORAN. Senator Hassan.

STATEMENT OF HON. MAGGIE HASSAN,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Thank you, Mr. Chair. And I want to thank you and Ranking Member Blumenthal for having this hearing today.

And thank you to our witnesses for being here.

When Mark Zuckerberg testified in April, I raised concerns about Facebook's business model resting on two potentially problematic foundations: maximizing the amount of time people spend on its products, and collecting and exploiting people's data. So, I was interested to see, and now hear, that all three of you, in your testimony, independently referenced problems inherent in Facebook's business model. Facebook's own corporate financial statements make it clear that what is best for the company is not always what is best for its users. That is part of why we have seen so many problems like the ones we are talking about today. The economic incentives for these companies are so strong that we simply cannot expect that these companies will always do the right thing by their users.

As I said at the time to Mr. Zuckerberg, I certainly believe in free enterprise, but, when private companies are unwilling or unable to do what's necessary to protect their customers and, frankly, individual rights in a democracy, public officials have historically stepped in, across a range of industries, to protect their constituents.

So, I'd like to take this time to ask all three of you—you've touched on it in your testimony, but to comment broadly on the inherent problems with Facebook's business model, and whether they require legislators to create some level of guardrails to protect consumers, including strong financial penalties, to change these companies' economic incentives.

And, Dr. Kogan, why don't we start with you, and then we'll go to Mr. Soltani, and then Mr. Battelle can bat cleanup.

Dr. KOGAN. Thank you, Senator.

I agree with everything you just said. I think it's pretty clear that Facebook is in the business of trying to keep you on Facebook as long as possible, because then they could serve you more ads. This is interesting, in terms of the contrast to Google, where they want you off as quickly as possible. That's their success rate, because——

Senator HASSAN. Yes.

Dr. KOGAN.—you've found the information you want. So, in that sort of situation, the model does run counter to not only our privacy, but our well-being, because the more you're spending time on your phone, the less time you're spending in nature or doing mean-

ingful work or interacting with people in a more genuine way. I think that's all concerning.

From a privacy perspective, as we have tried to educate ourselves about what are the current ways that Facebook and app developers use it and people interact with their apps, it's pretty amazing that, to this day, many apps have terms of service that either don't exist, run counter to Facebook's own policies.

Senator HASSAN. Yes.

Dr. KOGAN. In many places, it's actually difficult to find the terms of service, where, when you authorize an app, the terms of service are way on the bottom——

Senator HASSAN. Yes.

Dr. KOGAN.—in hard-to-read fonts, really small. On mobile, we've even found times when you're not even presented with the terms of service. So, this all goes back to the idea of consent. And when people—are we getting true consent? And I think the Facebook platform has been set up in a way that runs counter to true informed consent, and folks aren't being given the ability to choose wisely.

Senator HASSAN. OK, thank you.

Mr. Soltani.

Mr. SOLTANI. I think, absolutely, policy is—policy interventions are important here. I worry a little bit about focusing on consent a bit too much, because if you—it's hard to have meaningful consent if you predicate access to the service based on that consent. So, if I'm prevented from using the service, and I need the service for a number of features, is consent really a choice? And we see this in the GDPR cookie-click-in——

Senator HASSAN. Yes.

Mr. SOLTANI.—model.

Senator HASSAN. Yes.

Mr. SOLTANI. I hope to author a California ballot initiative that should be on the ballot in November. And one of—two of the key points there are that, while it does allow companies to monetize data on a first-party basis, it requires that companies allow consumers to opt out of any third-party sharing or sale of their information.

Senator HASSAN. OK.

Mr. SOLTANI. And it prohibits companies from denying them access to the service. So, you can monetize, but just monetize in a way that doesn't expose me to the harm.

Senator HASSAN. OK.

Mr. SOLTANI. I think focusing too much on just notice and giving consumers choice, it's kind of like food safety. Right? So, we can give people choices, but food can't contain arsenic.

Senator HASSAN. Right.

Mr. SOLTANI. Right? It can have different—and I think the same is true for this space. We need to give them choices, but there need to be some baseline protections.

Senator HASSAN. Thank you.

And Mr. Battelle.

Mr. BATTELLE. The advertising model that Facebook employs is not new to Facebook. What's new is how good they are at employing it. And I think what has been revealed in the Cambridge story

is how little consumers understand that model, and, frankly, how little regulators do.

Senator HASSAN. Yes.

Mr. BATTELLE. I think we need to educate ourselves. But, I think the idea that we should inhibit advertisers' ability to communicate with their customers should—we should tread lightly there.

Senator HASSAN. Yes.

Mr. BATTELLE. Because that is about free speech and also about commerce. So, we have to be careful.

Senator HASSAN. Thank you very much.

Thank you, Mr. Chair.

Senator MORAN. Senator, thank you.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much.

Thank you, to all of you. I'm on both the Judiciary Committee, this one, and I'm the Ranking on the Rules Committee, where we're going to have a hearing on some of this, touching on this, tomorrow.

But, my first question is about how we fix some of this, going forward. I'll ask you, Mr. Soltani. And Senator Kennedy and I introduced—there are a number of bills out there, but we introduced a bipartisan bill that would make privacy disclosures more transparent. It would give consumers the right to control their own data by allowing people to opt-out. And then, of course, requiring notification of data breaches in 72 hours. So, I mean, there has always been this philosophy that somehow the companies are going to police themselves. When Mark Zuckerberg testified here, he actually said he thought that we might need regulation now, which was quite a change in position.

Could you talk about why Federal legislation is necessary, and if you think some of this would be helpful?

Mr. SOLTANI. OK. Thank you, Senator.

While I haven't read the specifics of your proposal, the principles that you provide are, I think, incredibly necessary and incredibly important. I think consumers need to have the ability to essentially enact meaningful choice, but, again, there needs to be some baseline protections around data sharing, data breach, opt-out. Again, I worry about overly focusing on consent rather than providing protections. I do agree that we need innovation and we need to allow advertising and other business models to flourish, but I think we want to make sure that those are industries that are flourishing in an ethical way and not, kind of unabashed.

Senator KLOBUCHAR. Our bill would also establish remedies for consumers when a privacy violation occurs, including the right to prohibit further collection of personal data, have the operator erase all personal data that has been collected, cease further dissemination of personal data, and offer the consumer a copy of their data that has been collected. Do you think that would be helpful?

Mr. SOLTANI. I think, absolutely, injunctive relief and articulable harms are two critical pieces for any privacy initiative. I wonder if overly focusing on data portability is also an issue. Again, there's

this belief that being able to take your data from platform A and take it to platform B is beneficial, but, from a security perspective, you're basically increasing the likelihood of a data breach for each platform. Right? So, I think, in addition to data portability, we need strong requirements of data security and data safeguards on each platform.

Senator KLOBUCHAR. OK. Thank you.

Mr. Battelle, you brought up the issue of elections, I think, some. Is that right? OK. So, the Honest Ads Act is another bill that I'm doing with Senator McCain and Senator Warner. And that would look at what happened in the last election, where there was, like, no disclaimer requirements, and there were no disclosure requirements, and basically say you have to have the same rules of the game that you have if it's an audio ad, for radio, if it's a TV ad, for TV, if it's a print ad, for print. And I don't think it's that hard. And actually, some of the companies now, for some reason, are doing it on their own, which we truly appreciate. But, again, we're going to have a patchwork of rules if we just allow them to do that, because they're all doing it differently. So, could you comment about that?

Mr. BATTELLE. I, along with, I think, Facebook, Twitter, and Google, are—I'm a fan of the Honest Ads Act. I do think we have to, as, you know, we often dance on the head of a pin when it comes to definitions, issues-based ads. It gets squishy, and oftentimes there are issues-based ads that have nothing to do with election processes, and they may want to run when there happens to be an election.

Senator KLOBUCHAR. I do understand that there's a standard. It's easy to say that, although there is a actual standard set, by law——

Mr. BATTELLE. Yes.

Senator KLOBUCHAR.—that says it has to be an issue of national legislative importance. And actually, that is a standard that somehow my radio station in Thief River Falls, Minnesota, has to follow and figure out. So, my position is, I don't know why the biggest companies in America can't figure it out.

Mr. BATTELLE. And I think they can. I'm not sure if the smallest companies in America can.

Senator KLOBUCHAR. Well, my radio station in Thief River Falls is pretty damn small, so——

Mr. BATTELLE. Yes, I——

Senator KLOBUCHAR.—I mean, because there are all of these radio stations, print, and little TV stations that have had to figure this out——

Mr. BATTELLE. Right.

Senator KLOBUCHAR.—for years.

Mr. BATTELLE. And they have——

Senator KLOBUCHAR. They've been able to do it. And then, they keep the ads on file so that other campaigns—opposing campaigns can see them, so that journalists can see them, so we have some modicum of transparency in our democracy.

Mr. BATTELLE. Absolutely. I think——

Senator KLOBUCHAR. Because——

Mr. BATTELLE.—all of this has made——

Senator KLOBUCHAR.—people like to get off with saying, "Oh, you don't need issue ads," but they've been doing this for years.

Mr. BATTELLE. No, I think you absolutely do.

Senator KLOBUCHAR. OK.

Mr. BATTELLE. I want to make sure I'm clear on that. The only issue I have is with small business, which, with this kind of technology in advertising now, there are literally hundreds of thousands of kinds of ads they may need to screen, even if you are a two-person shop with a blog in Minnesota. And so, we want to make sure we don't make it impossible for those small businesses to also benefit from that kind of advertising.

Senator KLOBUCHAR. All right.

And then, I'll put some questions on the record on something that's been raised about the size of some of this, and the changing with antitrust law. And I'm—also happen to be the Ranking on that committee. So, Senator Lee and I are having a hearing coming up, but we also—this idea of how our laws work when you have changing circumstances with communications companies is something I think we need to look at. So.

Thank you very much.

Senator MORAN. Senator Klobuchar, thank you.

Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you very much, Chairman Moran.

And thanks, to all the witnesses, for being here. I think you've given some excellent testimony here today and helped enlighten us in this area.

We now live in a world where we're waiting to find out who else Facebook has allowed to access our data without our consent. Over 60 device manufacturers had access to some part of Facebook's data. And it's unclear how many third-party developers also had access to this data, and who they shared it with. The American public trusted Facebook with personal and intimate information, and it broke its trust. Facebook is not a trusted steward. And its negligent behavior that has allowed countless political ads filled with misinformation from foreign entities is having a direct impact on our democracy. This must stop, and it must stop now.

We have seen a great deal of public and congressional attention to these issues since the 2016 election, but we are going to see history repeat itself unless we have action. And I'm concerned that the Federal agencies with a role, here, the Federal Trade Commission or the Federal Election Commission, or both, are not doing enough to protect our privacy and our democracy.

Mr. Battelle, during the April Facebook hearing with Mr. Zuckerberg, I asked him to commit to advocate for the Honest Ads Act. He assured me that the most effective thing he could do was implement the bill's policies on the Facebook platform. Since Facebook implemented its version of political advertising transparency, we've seen the break-things-and-move-fast culture doesn't work for elections. The *New York Times* reported that ads promoting news articles about politics were being categorized as polit-

ical advertising. What impact will this change have on the reach of political journalism for the 2018 elections?

Mr. BATTELLE. I think the fair answer to your question, Senator, is, we don't know. With much of this technology, it is true that the executives and product managers behind it don't spend a lot of time thinking about scenarios that they don't want to happen. Instead, they spend most of their time thinking about what they wish to affect. And, in the case of a technology company like Facebook, that often has nothing to do with the impact on society, beyond either engagement of the user, if you're on a product team, or engagement for advertising, if you're on the advertising team.

I think what Facebook, as a company, is beginning to learn is how to be responsible beyond its primary edict of either making money or creating engagement. So, I think it's learning in realtime. I have seen friends of mine who are in senior positions at Facebook actually struggle with these questions in very honest ways. However, I do not believe that Facebook alone is capable of solving this problem.

Senator UDALL. Yes. What more can Facebook do to improve the transparency around political ads?

Mr. BATTELLE. Absolutely, Senator.

Bring in a panel—a heterogeneous panel of academics, experts, political scientists, journalists to help advise them as they make product choices. This is anathema to the ways Silicon Valley companies traditionally create product, but this is fundamental to our democracy. And they are beginning to do that, and I think they need to be held to account to ensure they continue to do that.

Senator UDALL. Mr. Battelle and Mr. Soltani, what actions do you support by Congress, the Federal Election Commission, or the Federal Trade Commission to tighten and enforce rules to stop the election meddling we saw in 2016?

Mr. SOLTANI. So, I absolutely agree that the Honest Ads Act is a good first step.

Senator UDALL. So, you support it.

Mr. SOLTANI. I do support it. I think one of the issues resulting from this whole debacle isn't necessarily about the effectiveness of the advertising or how well Cambridge Analytica's techniques work, but it's the undermining of trust in our news and fact-finding ability online. And what I haven't seen is, you know, how any of the interventions will address restoring public trust in both our news and journalism efforts, as well as our public Internet. So, I'd love to see something to try to address those pieces.

Senator UDALL. Yes.

Mr. Battelle, I'm actually out of time, so maybe you can help me with that one for the record. I'm going to submit additional questions for the record on, especially, specific kinds of action, whether you support it or not.

Thank you——

Mr. BATTELLE. I'd be happy to.

Senator UDALL.—very much, Mr. Chairman.

Senator MORAN. Thank you, Senator Udall.

Senator Blumenthal.

Senator BLUMENTHAL. Mr. Soltani, the record before us today and in our previous hearing seems to leave no doubt that Facebook has violated its consent decree. Would you agree?

Mr. SOLTANI. It is my opinion that they have, yes.

Senator BLUMENTHAL. And the only question now is what should be done about it. Under the terms of that consent decree, Facebook was required to establish a comprehensive privacy program to address privacy risks and obtain audits to ensure that the privacy of consumer information is protected. It did virtually none of those tasks. And, in fact, in testimony before us, sitting exactly where you are, Mark Zuckerberg said, in response to the question, How many other Cambridge Analyticas are there out there?—"We don't know." And, to my knowledge, they still don't know. So, the audits, the tracking of—or the oversight that Facebook was supposed to be doing simply has gone unperformed.

Are there other data collection or sharing practices that you believe warrant investigation by the FTC, as well?

Mr. SOLTANI. I'd have to think on that quite a bit, Senator, but I'm happy to respond, if—via written response——

Senator BLUMENTHAL. I would appreciate your doing so, because I, for one, will be strongly urging the FTC to go beyond the obligations of the consent decree. In other words, not only seek injunctive relief as to that decree, but also go beyond it, in further investigation that may go into the tracking of consumers—I'm sure you're familiar with that practice—monitoring private messages for advertising purposes, monitoring third-party websites. You're familiar with all those practices, are you not?

Mr. SOLTANI. I am, yes.

Senator BLUMENTHAL. Do you believe they warrant investigation?

Mr. SOLTANI. I believe some of them have been investigated. I know, for example, monitoring private messages has—there are some private cases on that fact in—that might be settled in California. I'm not certain. But, I believe all of those deserve scrutiny, yes.

Senator BLUMENTHAL. Speaking of audits, Professor Kogan, are you aware of any forensic audits conducted by Facebook of Cambridge Analytica?

Dr. KOGAN. I believe they tried to do one, but then the ICO kicked them out.

Senator BLUMENTHAL. In other words, they failed to do it.

Dr. KOGAN. So, my understanding was, they were about to do it, but then they were stopped because the ICO, which is the Information Control in England, wanted to do it first.

Senator BLUMENTHAL. What about of your app?

Dr. KOGAN. They have not.

Senator BLUMENTHAL. They have not. Have they ever asked?

Dr. KOGAN. They asked at the beginning of the controversy, in March, but then they simply went away.

Senator BLUMENTHAL. They disappeared.

Dr. KOGAN. They disappeared.

Senator BLUMENTHAL. Probably not a good sign of compliance with the FTC consent decree, would you agree?

Dr. KOGAN. I am definitely not an FTC lawyer, so I'll have to abstain from making a judgment.

Senator BLUMENTHAL. Well, I can tell you, it's not a good sign. [Laughter.]

Senator BLUMENTHAL. Do you have a nondisclosure agreement with Facebook?

Dr. KOGAN. I have, but I believe they've waived it so I could speak freely.

Senator BLUMENTHAL. So, they imposed a nondisclosure agreement, but then waived it when it became clear that, in effect, you were wanting to tell your side of the story.

Dr. KOGAN. I think that is correct.

Senator BLUMENTHAL. There has been a reference—I think I made the first reference; Mr. Battelle, you also noted it—the GDPR. I think you spoke somewhat disapprovingly of the idea that our country might follow that lead. I happen to believe that those sorts of standards are the minimum that we should be adopting, and that those kinds of standards are essential for the consent—informed consent, clear consent—that amounts to permission, not forgiveness—we ought to be insisting that Facebook and others adopt, as well. Could you tell me why you think that view is mistaken, if you do?

Mr. BATTELLE. I'm actually a fan of the intent of GDPR. I am not a fan of what happened after it was implemented, which is that all the large firms, which have the lawyers, the staff, the resources, and the ability to bring compliance between you and the next picture of a baby—"Hey, by the way, do you agree to this?" and you hit "OK" to get rid of it so you can see, you know, your neighbor's baby photos; whereas, very small companies do not have the ability to do that kind of compliance. So, GDPR, what I disagree with is not the intent of the regulation. I disagree with how it's implemented and how it actually allows large companies to grow larger and have larger moats around them, which leads to an oligarchy of data controllers. That's my objection.

Senator BLUMENTHAL. Are there conditions or other kinds of provisions that would, in effect, protect against that unintended consequence?

Mr. BATTELLE. I believe they are, and I'd be happy to go further into it in written testimony.

Senator BLUMENTHAL. I would appreciate that very much. I'm not advocating that we follow the GDPR simply because it's there. If we can improve on it, so much the better. And talking about the threats of bigness and monopolistic power, I think that is an area that we need to be intently aware of. It is a threat and a challenge, along with others. It's not the reason that we're here today, but it certainly has to be a concern, and I'm glad that you raised it.

I'm going to yield here, Mr. Chairman, and thank, again, the Chairman of the Committee, Senator Thune, for his leadership in this area. And I'm glad that he's with us.

Senator MORAN. Thank you, Senator Blumenthal.

Just before I turn to Senator Thune, I would welcome the input. Senator Blumenthal indicated, earlier, he's in the process of drafting legislation of privacy bill of rights, and he indicated an interest in GDPR. We're in discussions about joining him in that effort,

with a number of other Senators. I would welcome any input that you would have. I was going to, particularly, ask you, Mr. Battelle, about your concerns about GDPR, in light of what Senator Blumenthal said in his opening statement, but I think you've responded to that, and indicated you're going to respond further. But, if there's a way that you believe that, legislatively, we can get at this, I would welcome that input as Senator Blumenthal and I work on this topic.

Senator MORAN. We're pleased to have the Chairman of the Full Committee join us, and I now recognize Senator Thune.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Thank you, Chairman Moran and Ranking Member Blumenthal, for holding this important hearing, which follows up on our April 10th full-committee hearing with Facebook CEO Mark Zuckerberg.

And I would also echo what you both have just said with respect to the thoughts that you might have about GDPR. That is something that gets a lot of discussion. It's obviously something that's been reported on a lot by the media in this country. But, as we look at potential solutions, we would certainly like to look at things that, perhaps, are good, that work in that format, that structure, and avoid those things that would not be helpful. So, we're very interested in your perspective on that, and suggestions that you might have about how we, if we need to, might proceed here.

The hearing on Facebook gave us an opportunity to look at the company's conduct and the corrective actions that it has taken, or that it plans to take. And I think this hearing gives us an opportunity to continue that examination and figure out what went wrong at Facebook, and how similar problems might be avoided in the future. And, while Facebook remains under the microscope, we should also consider how the collection and use of consumer data across the entire social media landscape impacts competition, how it impacts consumer welfare, and how it impacts consumer privacy concerns. And so, I thank all of you for appearing today to shed light on those subjects.

And I want to ask—Mr. Kogan, you testified that, when Facebook users who participated in your survey logged into Facebook through the GSR app portal, Facebook presented a link to the GSR app's terms of service. These terms of service stated, "The participants permit GSR to transfer or sell the data for any purpose, and that GSR may collect demographic data and Facebook Likes from participants and their network." So, the question is, Did you and Facebook enter into an agreement or contract limiting in any way your ability to collect, use, or transfer Facebook user data? And, if so, when and how?

Dr. KOGAN. Thank you, Senator.

So, the experience of making an app on Facebook, I think, is really helpful in understanding this. The experience is very similar to signing up for Facebook, where you don't talk to any human being, there's no contract that you really engage in. You just simply go in the portal and say, "I want to develop an app," and then you create the app, and away you go. The first time that I could really

recall having any interaction with a human being on the Facebook side was in December 2015, when that first *Guardian* article reported about the project. So, that was a year and a half later.

The CHAIRMAN. OK. At what point did you become aware that GSR's terms of service conflicted with Facebook's policy regarding the transfer of Facebook user data from app developers to third parties such as Cambridge Analytica?

Dr. KOGAN. So, the honest answer is, I'm not 100 percent sure. Reviewing our records, the best I can find is the spring of 2015, and at which point we got some counsel on the terms of service after we started to worry a little bit about Mr. Wylie's advice. And he pointed out that discrepancy. We were also advised, at that point, that Facebook's policy is not really its policy, for a variety of legal reasons that I'm probably not qualified to state. And so, that raised concerns, and we went through various ways of letting Facebook know, because I had a relationship with them as a researcher.

The CHAIRMAN. So, I guess that's that—the next question I had, and that is that, What actions, if any, did you take once you learned of the conflict? And you—sounds like you said you——

Dr. KOGAN. Yes. So, there are a couple of things that happened. First, we had an active research collaboration with Facebook, and they visited me sometime in 2015. And during that meeting, I talked a little bit about it. There was no real indication of anything that was worrisome. Also, my partner on the project was interviewing for a job at Facebook, and my understanding is, he disclosed to Facebook during the interview about the project. And I don't believe there were any objections that were raised.

The CHAIRMAN. Did you and Chris Wylie discuss the GSR terms of service and Facebook's privacy policies? And, if so, when?

Dr. KOGAN. So, when we——

The CHAIRMAN. And maybe describe the substance of those discussions.

Dr. KOGAN. Yes, of course. So, my app, originally, was just an academic app. I was using it for my lab. So, when we started the relationship with SCL, I obviously had concerns about making sure I was on fully commercial terms. So, Chris provided the assurance that, "Hey, I'm a DEDA lawyer, and I'm going to walk you through this process." And so, at that point, I kind of handed off the reins to him. Then, I believe, in early June 2014, he sent me the terms of service that he wanted me to put in the app, and asked me just to fill in our address.

The CHAIRMAN. OK.

Dr. KOGAN. And so, we did.

The CHAIRMAN. Did you discuss with him whether the GSR terms of service in any way conflicted with Facebook's privacy policies, such as those relating to the transfer of Facebook user data to third parties?

Dr. KOGAN. I have no recollection of such a conversation.

The CHAIRMAN. OK.

This I would direct to all three panelists. But, maybe you could just speak to the question of, What specific steps do you believe that Facebook still needs to take to ensure that its users' data is not collected, used, or transferred without users' informed consent?

Mr. BATTELLE. Yes, I'd be happy to——

I think the thing that we often forget is, as consumers, anything that pops up in between us and something we want is annoying, and we want it to go away as quickly as possible, even if it happens to be something that's actually quite important or good for us in the long run. This requires that we actually apply user design in all the insights that engage us to inform us about things that perhaps are a bit more longer-fused than, you know, just getting to the next photo or making the next Tweet. So, I believe what we need to do is work with industry to understand how to integrate that into the product design flow so that at the moment at which data may be given up, you are reminded of the possible implications of that, as opposed to just asked to dismiss a modal dialogue box with an "OK" button.

The CHAIRMAN. Anybody else? Mr.—yes—Soltani, you want to——

Mr. SOLTANI. So, I think that's an important step. One of the challenges is that, with mitigating risk, kind of, behavioral economics tells us that people are really bad at estimating risk. Right? So, I could tell you that, "By driving this car, you're likely to get in a car accident, but we think that's a low-probability event," and we have a hard time articulating or guessing what the probability of harm is, so we're going to discount it and we're not going to wear our seatbelt. So, instead, we say, "You know what? You need to wear a seatbelt," and that might seem paternalistic, but that works to deal with our human assessment of risk, because we're bad at it.

The other piece, I think, that's challenging here is, we—a lot of the online services, whether it's Facebook or mobile apps or, you know, apps on our browser—browser extensions—we have a hard time differentiating between what is Facebook, what is the *New York Times,* and what is Mr. Kogan's app. Right? Oftentimes, these bleed in together with similar branding, similar, kind of, look and feel. And so, we're not quite sure who we're disclosing information to, or we might feel that, because Facebook invited this person onto our browser, we should trust this person. It's like if—as if I invite you to a dinner party, and then you invite your friends——

The CHAIRMAN. Right.

Mr. SOLTANI.—and you're basically vouching for them, but, in fact, you just picked the guy up on the street and let him into my house. Right? That's essentially what we have.

The CHAIRMAN. Mr. Kogan.

Dr. KOGAN. So, I think my co-panelists have made a lot of really excellent points. The one thing I would just add to it is, I think we need to shift away from this idea of blanket consent to informing people about the particulars. Because when you say that, you know, "I grant you the right to do whatever you want with my data," that sets up a situation where you may do something I don't like, I just haven't anticipated it. So, I think the more Facebook can be transparent about the specifics of what they want to do with the data, the fewer bad surprises the consumer is going to find.

The CHAIRMAN. Right.

Final question, Mr. Chairman. What specific changes in industry practices generally would you say are most needed to protect consumer privacy? And again, that could be to any or all of you.

Mr. SOLTANI. I think, data sharing without affirmative consent.

The CHAIRMAN. OK.

Mr. BATTELLE. I'm a very large fan of giving consumers a dashboard, where they understand, across apps, across services, the power and value of their own data, and enabling that dashboard to be used as currency by the individual, as opposed to by the company. Right now, most of the data control exists up in the platform level and not down at the individual level. This would require a coordinated effort across industry, but I think it would enable an innovation economy we have yet to see.

The CHAIRMAN. OK.

Mr. Kogan?

Dr. KOGAN. So, the one thing that is often missed in Silicon Valley is that not everything and every technology that is used actually betters people's lives. There is a belief that it does, but I think Facebook is a—is kind of a classic example, where what they're trying to achieve is more of an addictive pattern of behavior, rather than one that supports things that we usually value as human beings, such as happiness and relationships and doing meaningful work.

So, I think more honest and sobering thought about how we run our businesses. And when the key benchmark that is used to indicate success—and John pointed this out—runs counter to the things that folks really strive for, and you're creating a platform that is really an addictive platform, I think we need to have a really serious check on that and a hard conversation about, How do we regulate either ourselves or from the government on checking that effect?

The CHAIRMAN. Mr. Chairman, to be continued. Thank you all very much.

Senator MORAN. Mr. Chairman, thank you.

Let me ask just a few concluding questions. Ah. Let me not, at the moment, ask a few concluding questions.

[Laughter.]

Senator MORAN. Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO, U.S. SENATOR FROM NEVADA

Senator CORTEZ MASTO. Thank you. Thank you, Mr. Chair and Ranking, for holding this.

And thank you for those—the conversation. I appreciate you being here. And I want to follow up on the discussion that you've been having with Chairman Thune.

Let me ask you this. As legislators, what should we be thinking about to verify that, when Americans are told that their data has been destroyed, that deletion can actually be confirmed? What do we—what should we be doing, if anything, or how can we help to assist that determination? And I'll open it up to the panel.

Dr. KOGAN. So, the first thing I'll say is, it's almost impossible for that to be true and to know. So, the problem with the whole audit idea is that it will only catch good actors who are interested

in doing the right thing. So, imagine I have some Facebook data, I say I deleted it. And audit will catch only the things I missed by accident.

But, if I'm a bad actor——

Senator CORTEZ MASTO. Right.

Dr. KOGAN.—I could take that data, put it on a hard drive, and stick it under my mattress. Facebook will never catch that. And so, I think the idea that audits are going to solve any of this is a little ridiculous, to be honest, because if the worry is about the bad actors, it's going to do nothing to actually stop that.

Senator CORTEZ MASTO. Any other comments?

Mr. SOLTANI. I just want to echo that I think it's unreasonable to think that data, once out there, can be called back. Right? And I think that the issues that we see around personal data are not unlike the issues we see with copyright, which is that, you know, someone can take information that's put out there and create a copy of it, and then do with it—so, we then have fines and impose penalties for possessing an illegal copy, but it's not perfect. Right? Because someone can always, kind of, copy it and put it on their—so, I think it's difficult to think that we can call back data.

Senator CORTEZ MASTO. Right.

Mr. BATTELLE. I agree with that. I think that how data is used and the framework in which it can be legally and appropriately used needs to be truly understood and enforced. There is a massive gray and black-market in information. I mean, the Equifax breach, for example, when my wife asked if we were breached, I said, "Oh, don't worry, I already had the security clearance breached 2 years ago. Everything's out there. There's nothing new to be seen here. We're already in black—in the files of the Dark Web." So, the question is, How will that information be used inappropriately and to protect ourselves from the inappropriate use, as opposed to presume that a data audit is actually going to claw back.

Senator CORTEZ MASTO. Uh-huh, please.

Mr. SOLTANI. Actually, if I may, there is a somewhat convoluted, but potential combination of the two comments, which is that you could reward good actors that can demonstrate that the data was collected in a, kind of, ethical or a consensual way. And this is what Facebook is attempting to do with its data partnerships with the data brokers that it's working with as it clawed back its policies. It said, "You need to promise us that you got these e-mail addresses in a legitimate way." Whether those promises are true—but, you can say certain actors that can have an—essentially, a duty to prove to you that the data was collected responsibly receive certain benefits or certain safe harbors, and then the other actors kind of operate in a gray market, and always will, but we would, hopefully, see them kind of diminish over time.

Mr. BATTELLE. I would just add that we have seen this happen in this industry over many years. There was an extraordinary gray market in search advertising and in data around that. And, through industry collaboration, that was cleaned up. The ethical source of—sourcing of data is a concept that's relatively new, I think, in the public discourse, but it is not new at all to actors who have been in this business for decades. It is literally how they make their living. And I think ensuring that those actors are thor-

oughly audited and accredited, and that their trust is earned on a regular basis, is really important. And I think we've seen that trust lost, in some cases, but I think we need to also ensure that that trust is established so that we can trust these third parties who are the, you know, ethical stewards of this information.

Senator CORTEZ MASTO. Thank you. Thank you. I'm—very, very enlightening. And that's what I think we all wanted to hear.

I have one follow-up question. And this goes to the subject matter. So, I had the opportunity to serve as the Attorney General of Nevada, and I know there's—has been a discussion over the right balance between working with our law enforcement and sharing information and data and opening up to investigations. So, would you comment on the factors that companies should keep in mind as it pertains to keeping sensitive data and ensuring that they can appropriately assist investigations that may follow? Do you have any comment on that?

Mr. SOLTANI. None, really.

Dr. KOGAN. Sounds like a minefield.

[Laughter.]

Senator CORTEZ MASTO. Right.

Mr. BATTELLE. This is a minefield, and this is the subject of some of my current work, which is, you know, the appropriate use of information in the social architecture of data in our society. I think the discoverability that the data exists is important. Whether or not the data is shared has to be, you know, through a process of legal review. I mean, it has to be auditable and appropriate, and, if a mistake is made, it needs to be corrected immediately. So, I'm a very big fan of sharing data between agencies, between law enforcement, but in an appropriate framework. And I think that we've seen inappropriate frameworks that has been discovered through the free press, frankly, after 9/11, as one example.

Senator CORTEZ MASTO. Right.

Mr. BATTELLE. And I think we have to be very careful. It is a minefield, but the——

Senator CORTEZ MASTO. But, it's a conversation we should have. We——

Mr. BATTELLE. It's absolutely a——

Senator CORTEZ MASTO.—need to have——

Mr. BATTELLE.—conversation——

Senator CORTEZ MASTO.—this conversation so we can——

Mr. BATTELLE.—we should have. I believe so, yes.

Senator CORTEZ MASTO. Thank you.

Thank you.

Mr. SOLTANI. I mean, under the third-party doctrine, pretty much my understanding is, everything collected by companies is available to law enforcement. Right? And so, I think a good question for society and folks, you guys as regulators, is that, as nearly all of our communications go through—mediated through third parties, is that a world we want to live in? I think that's important.

Senator CORTEZ MASTO. Yes. Thank you.

Thank you very much.

Senator MORAN. Senator Blumenthal is offering the opportunity for him to go ahead of me, but, knowing——

[Laughter.]

Senator MORAN.—but, knowing that there are votes in 10 minutes, I'm going to go next, and then will recognize Senator Blumenthal but, I think we'll have time for both of us, or all of us.

I'm also a member of the Appropriations Committee, and I'm on the Subcommittee that funds the Federal Trade Commission. So, maybe beginning with you, Mr. Soltani, tell me about the resources that you believe the FTC has, particularly in the Office of Technology, Research, and Investigation, and the staffing that should be required to perform their duties in regard to this—protecting consumers in this Digital Age. Where are we?

Mr. SOLTANI. I think that's an excellent question.

I was the second technologist at the FTC, so, prior to me, one other person had been there for a few months, and, prior to that, with the exception of hiring experts on specific investigations, they did not have technologists. Right? And part of the reason why we saw—so, I worked on Google, Facebook, Twitter——

Senator MORAN. When did you depart?

Mr. SOLTANI. So, I was there from 2010 to 2011, and then I came back in 2014 to establish the Office of Technology Research.

Senator MORAN. OK.

Mr. SOLTANI. And I think what became apparent is, as more and more of these investigations were technical in nature, such as APIs and how APIs work or how advertising networks and realtime bidding works, it became apparent that the agency—and it's kind of yourselves, as you hire technology fellows, that technologists are incredibly important in deciphering and understanding how these systems work and figuring out where the boundaries are. And I would say—so, in my time there, we set up the Office of Technology Research. And it was staffed with, I think, at the end, about six people, total. I think it's about that size, maybe down one person. But, I think, moving forward——

Senator MORAN. Now?

Mr. SOLTANI. Now. I think, moving forward, in the same way that economics—and the FTC has a Bureau of Economics that basically weighs in on nearly every consumer protection and every consumer competition case, BCP and BC always has an economist. I think it's important to make sure that there's an equivalent Bureau of Technology that weighs and both understands how technology and privacy work and security work, but also around some of the network effects, some of the economics, some of the platform dominance effects in the same way that the economics group does. So, I think giving the agency the resources to expand that and perhaps make it into its own bureau would be, I think, a huge benefit, both to the FTC as well as society at large.

Senator MORAN. Somewhat in that regard, how does the FTC—I—you may know this, Mr. Soltani, you may not, but how does the FTC monitor, in this case, Facebook's compliance with the consent decree? What's the process that takes place, once the consent decree is entered, to see that it is complied with?

Mr. SOLTANI. I can't speak directly to that. I can point you to some public academic research that's examined that process and, in that—kind of, in that research, some key points highlighting the difficulty in, essentially, reviewing, kind of, these compliance audits

that come to the agency. So, I can point you to that in testimony later——

Senator MORAN. Thank you.

Is—to all three of the panelists, are we really talking about specific criticism of Facebook? Is it any different or unique from other entities in the business of sharing data?

Mr. BATTELLE. Yes, everyone looks at me. It is unique. However, there are many, many companies that have, you know, significant stores of data that are, I think, equally as powerful, but different. Amazon knows everything you've bought. Google knows what you're interested in. There are many large companies, for example, in the genetics and medical field who have extremely sensitive information. And, of course, in financial services, as well.

Now, there is a—there is, you know, highly embroiled law around health and financial services. There is not, around these technology firms. What's unique about Facebook is the sort of jet-fuel-powered business model that drives it, that is based on the personal information that you give to Facebook. Google is similarly driven; however, Google is not a social network, per se.

I would say, if you would like to look at what is the most similar between companies like Google and Facebook, look at YouTube. YouTube is very similar in its both engagement and in its advertising. So—and if you look at, for example, the ongoing investigations as it relates to the Russian interference in the election, there are a lot of dark holes to go down when it comes to YouTube.

And so, I would say Facebook's not the only player here, but it's the one that certainly we're all most familiar with and the one that has, certainly, the most personal information about people.

Senator MORAN. And Senator Markey's questions raised national security concerns. I think maybe this was with you, Mr. Battelle. And particularly where you were responding to his question about the consequences of a Chinese company that was one of the 60 mobile device manufacturers. Are there other areas of national security issues related to what we're talking about here today that we ought to be aware of, or that you're aware of?

Mr. BATTELLE. Well, I mean, the truth is, is that the integrations that were done with these companies early in the days of mobile, before a company like Facebook, which, at that time, was quite young, could afford to create an app for every single mobile device in the world. We should not forget that Gmail or any e-mail app did exactly the same thing with all of these device makers, as did most of the major, you know, applications—I mean, YouTube, calendar apps—anything that had to exist on a phone device, or a tablet device that needed to be integrated with it did very similar things that Facebook did. This was common practice across the technology industry, and is reflective of, again, the lack of foresight on the potential externalities that—you know, that might, you know, occur in a scenario where a company that may, you know, see this easy window into getting information from U.S. citizens, used that window. We don't know—and that's probably the most damning thing—we do not know, and nor do these app makers, whether it be Facebook, YouTube, or Gmail, or Hotmail, or Bing, for that matter. So, that's the thing is, we are just realizing that, in our headlong race to make things, you know, faster, cooler, bet-

ter, there were potential implications we did not consider as an industry.

Senator MORAN. Thank you very much.

With the expectation of votes shortly, Senator Blumenthal.

Senator BLUMENTHAL. As you can tell from the good-natured repartee here, this work is very bipartisan and very collegial. And I really just want to thank the Chairman and all of our witnesses for being here. This hearing has been extremely useful and important.

And I would like to follow up on your suggestion, Mr. Battelle, that we would benefit by continuing to consult with all of you, because you each bring separate skills and experiences.

I would just quote from your testimony, Mr. Battelle, a very cautionary and somewhat alarming note, "Given that data is nonrivalrous and services such as Facebook are free of charge, it is often presumed that there is no harm to consumers or, by extension, to society in its use." There may be grave consumer harms, not only in privacy, but, as you suggest, in monopolistic practices that antitrust law is designed to prevent. We ignore those perils at grave risk to ourselves.

And I think that I—personally, I have no pride of ownership or authorship in any bill of rights to protect privacy. A privacy bill of rights is a term, and we need to make it real in ways that are enforceable and, really, protective of consumers without unintended consequences.

So, I look forward to continuing this work and to making sure that we do protect the values of our society in all these ways.

Thanks, Mr. Chairman.

Senator MORAN. Thank you very much.

Senator Cortez Masto, anything you'd like to——

Senator CORTEZ MASTO. No, thank you.

Senator MORAN. OK.

First of all, let me do my usual practice of asking any or all of the witnesses if they have anything they would like to add to today's testimony to correct or respond or anything that you felt like you didn't have an opportunity to address at the end of the hearing. Anything you want to add for the record?

Mr. SOLTANI. Just one thing. Sorry.

Senator MORAN. Mr. Soltani.

Mr. SOLTANI. Just to your earlier question of, Is Facebook different? I think, as I mentioned in my written testimony, in addition to the—kind of, the privacy invasions that people experience on Facebook and around Cambridge Analytica, one of the outcomes of Facebook and a Facebook-like service is, it's driven the entire industry to an authenticated, real-name-based profiling and advertising. Prior to Facebook, a lot of online advertising was pseudonymous, based on cookies. They didn't know you by name, they just knew your browser and where you visited, and that was sufficient to target ads to you. Around 2009, with the growth of Facebook, companies like Google and others pushed to have real-name-based profiling and identification, and that trend's only grown.

And one thing I want to just kind of highlight is, as there is pressure for Facebook to deal with fake accounts and bots and other, kind of, Russian intervention, we want to be mindful that we don't

push a company, who has incentives to identify people by name, and require them to further identify and verify people's identities by using their cell phone, their driver license, et cetera. So, I want to just, kind of as a policy note, flag that, because I see a lot of the debates in this space go that way, and I want to just highlight that the need for anonymous speech or pseudonymous speech is still important on the Internet. We want to make sure that we address that.

Senator MORAN. Thank you.

I join Senator Blumenthal in thanking all three of you for your appearance here today. The testimony was valuable. The conversations that followed questions was very useful. I think this is one of our most important hearings that we've had.

I also would notice that—just note, in a compliment or recent observation of my—of the audience that we've had, this may be the youngest in age——

[Laughter.]

Senator MORAN.—of any congressional hearing that has occurred.

Senator BLUMENTHAL. Mr. Chairman, I take umbrage at that.

[Laughter.]

Senator MORAN. Just look at these people. So, we're delighted that our witnesses joined us, as well—I'm sorry, our audience joined us, as well.

Let me ask unanimous consent that the record include a statement from the Electronics Privacy Information Center be placed in the record. Without objection.

[The information referred to follows:]

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, June 18, 2018

Senator JERRY MORAN, Chairman,
Senator RICHARD BLUMENTHAL, Ranking Member,
Senate Committee on Commerce, Science, and Transportation,
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security,
Washington, DC.

Dear Chairman Moran and Ranking Member Blumenthal:

We write to you regarding the hearing this week on "Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks."[1] We appreciate your interest in this important issue. For many years, the Electronic Privacy Information Center ("EPIC") has worked with the Commerce Committee to help protect the privacy rights of Americans.[2] EPIC has also played a leading role at the Federal Trade Commission, bringing to the Commission's attention emerging privacy and civil liberties. And EPIC is the group that brought the complaint in 2009 to the FTC re-

[1] *Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks: Hearing Before the S. Comm. on Commerce, Science, & Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security,* 115th Cong. (2018), *https://www.commerce.senate.gov/public/index.cfm/2018/6/subcommittee-to-hold-hearing-examining-social-media-data-use-and-privacy-concerns* (June 19, 2018).

[2] *See, e.g., An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA): Hearing Before the S. Comm. on Commerce, Science, and Transportation,* 111th Cong. (2010) (statement of Marc Rotenberg, Exec. Dir. EPIC), (C–SPAN video at *https://www.c-span.org/video/?293245-1/childrens-privacy*), *https://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf; Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation* 110th Cong. (2008) (statement of Marc Rotenberg, Exec. Dir. EPIC) (C–SPAN video at *https://www.c-span.org/video/?205933-1/computer-spyware*), *https://www.epic.org/privacy/dv/Spyware_Test061108.pdf.*

garding Facebook's data practices that resulted in the 2011 Consent Order.[3] And EPIC is the group that sued the FTC for its failure to enforce a similar order against Google.[4]

In this statement we outline the history of the 2011 Consent Order, point to subsequent developments (including the recently disclosed user data-disclosure agreements with device makers[5]), and make several recommendations. Our assessment is that the Cambridge Analytica breach, as well as the disclosure of users' personal information to device makers, could have been prevented if the Commission had enforced the Order.

EPIC would welcome the opportunity to testify, to provide more information, and to answer questions you may have. Our statement follows below.

EPIC, the 2011 FTC Consent Order, and Earlier Action by the FTC

Facebook's transfer of personal data to Cambridge Analytica was prohibited by a Consent Order the FTC reached with Facebook in 2011 in response to an extensive investigation and complaint pursued by EPIC and several U.S. consumer privacy organizations.[6] The FTC's failure to enforce the order we helped obtain has resulted in the unlawful transfer of 87 million user records to a controversial data mining firm to influence a presidential election as well as the vote in Brexit. The obvious question now is "why did the FTC fail to act?" The problems were well known, widely documented, and had produced a favorable legal judgement in 2011.

Back in 2007, Facebook launched Facebook Beacon, which allowed a Facebook user's purchases to be publicized on their friends' News Feed after transacting with third-party sites.[7] Users were unaware that such features were being tracked, and the privacy settings originally did not allow users to opt out. As a result of widespread criticism, Facebook Beacon was eventually shutdown.

In testimony before the Senate Commerce Committee in 2008, we warned about Facebook's data practices:

> Users of social networking sites are also exposed to the information collection practices of third party social networking applications. On Facebook, installing applications grants this third-party application provider access to nearly all of a user's information. Significantly, third party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends and network members that the user can see. This level of access is often not necessary. Researchers at the University of Virginia found that 90 percent of applications are given more access privileges than they need.[8]

Nonetheless in February 2009, Facebook changed its Terms of Service. The new TOS allowed Facebook to use anything a user uploaded to the site for any purpose, at any time, even after the user ceased to use Facebook. Further, the TOS did not provide for a way that users could completely close their account. Rather, users could "deactivate" their account, but all the information would be retained by Facebook, rather than deleted.

EPIC planned to file an FTC complaint, alleging that the new Terms of Service violated the FTC Act Section 5, and constituted "unfair and deceptive trade practices." In response to this planned complaint, and a very important campaign organized by the "Facebook Users Against the New Terms of Service," Facebook re-

---

[3] *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), *http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.*

[4] *EPIC v. FTC,* 844 F. Supp. 2d 98 (D.D.C. 2012), *https://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf.*

[5] Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, *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.*

[6] Fed. Trade Comm'n., *In re Facebook,* Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012) (Hereinafter "Facebook Consent Order"), *https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.*

[7] EPIC, Social Networking Privacy, *https://epic.org/privacy/socialnet/.*

[8] *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation* 110th Cong. (2008) (statement of Marc Rotenberg, Exec. Dir. EPIC) (C–SPAN video at *https://www.c-span.org/video/?205933-1/computer-spyware*), *https://www.epic.org/privacy/dv/Spyware_Test061108.pdf.*

turned to its previous Terms of Service. Facebook then established a comprehensive program of Governing Principles and a statement of Rights and Responsibilities.[9]

As we reported in 2009:

> Facebook has announced the results of the vote on site governance. The initial outcome indicates that approximately 75 percent of users voted for the new terms of service which includes the new Facebook Principles and Statement of Rights and Responsibilities. Under the new Principles, Facebook users will "own and control their information." Facebook also took steps to improve account deletion, to limit sublicenses, and to reduce data exchanges with application developers. EPIC supports the adoption of the new terms. For more information, see EPIC's page on Social Networking Privacy.[10]

However, Facebook failed to uphold its commitments to a public governance structure for the company.

From mid-2009 through 2011, EPIC and a coalition of consumer organizations pursued comprehensive accountability for the social media platform.[11] When Facebook broke its final commitment, we went ahead with a complaint to the Federal Trade Commission. Our complaint alleged that Facebook had changed user privacy settings and disclosed the personal data of users to third parties without the consent of users.[12] EPIC and others had conducted extensive research and documented the instances of Facebook overriding the users' privacy settings to reveal personal information and to disclose, for commercial benefit, user data, and the personal data of friends and family members, to third parties without their knowledge or affirmative consent.[13]

We explained our argument clearly in the 2009 EPIC complaint with the Commission (attached in full to this statement):

> This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.[14]

We should also make clear that the 2009 complaint that EPIC filed with the Federal Trade Commission about Facebook was not the first to produce a significant outcome. In July and August 2001, EPIC and a coalition of fourteen leading consumer groups filed complaints with the Federal Trade Commission (FTC) alleging that the Microsoft Passport system violated Section 5 of the Federal Trade Commission Act (FTCA), which prohibits unfair or deceptive practices in trade.[15]

---

[9] *Facebook takes a Democratic Turn,* USA Today, Feb. 27, 2009, at 1B, *https://www.pressreader.com/usa/usa-today-us-edition/20090227/281887294213804*

[10] EPIC, *Facebook Gets Ready to Adopt Terms of Service* (Apr. 24, 2009) *https://epic.org/2009/04/facebook-gets-ready-to-adopt-t.html*

[11] There is a longer history of significant events concerning the efforts of Facebook users to establish democratic accountability for Facebook during the 2008–2009 period. The filing of the 2009 complaint came about after it became clear that Facebook would not uphold its commitments to the Statement of Right and Responsibilities it had established. It would also be worth reconstructing the history of the "Facebook Users Against the New Terms of Service" as Facebook destroyed the group and all records of its members and activities after the organizers helped lead a successful campaign against the company. Julius Harper was among the organizers of the campaign. A brief history was written by Ben Popken in 2009 for *The Consumerist,* "What Facebook's Users Want In The Next Terms Of Service," *https://consumerist.com/2009/02/23/what-facebooks-users-want-in-the-next-terms-of-service/*. Julius said this in 2012: "Most people on Facebook don't even know they can vote or even that a vote is going on. What is a democracy if you don't know where the polling place is? Or that a vote is even being held? How can you participate? Ignorance becomes a tool that can be used to disenfranchise people." *Facebook upsets some by seeking to take away users' voting rights,* San Jose Mercury News, Nov. 30, 2012, *https://www.mercurynews.com/2012/11/30/facebook-upsets-some-by-seeking-to-take-away-users-voting-rights/*.

[12] *In re Facebook,* EPIC.org, *https://epic.org/privacy/inrefacebook/*.

[13] *FTC Facebook Settlement,* EPIC.org, *https://epic.org/privacy/ftc/facebook/*.

[14] *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), *http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.*

[15] EPIC, *Microsoft Passport Investigation Docket, https://epic.org/privacy/consumer/microsoft/passport.html.*

EPIC and the groups alleged that Microsoft violated the law by linking the Windows XP operating system to repeated exhortations to sign up for Passport; by representing that Passport protects privacy, when it and related services facilitate profiling, tracking and monitoring; by signing up Hotmail users for Passport without consent or even the ability to opt-out; by representing that the system complies with the Children's Online Privacy Protection Act; by not allowing individuals to delete their account; and by representing that the system securely holds individuals' data.

We requested that the FTC initiate an investigation into the information collection practices of Windows XP and other services, and to order Microsoft to revise XP registration procedures; to block the sharing of Passport information among Microsoft properties absent explicit consent; to allow users of Windows XP to gain access to Microsoft websites without disclosing their actual identity; and to enable users of Windows XP to easily integrate services provided by non-Microsoft companies for online payment, electronic commerce, and other Internet-based commercial activity.

The Federal Trade Commission undertook the investigation we requested and issued an important consent order. As the Commission explained announcing its enforcement action in 2002:

> Microsoft Corporation has agreed to settle Federal Trade Commission charges regarding the privacy and security of personal information collected from consumers through its "Passport" web services. As part of the settlement, Microsoft will implement a comprehensive information security program for Passport and similar services. . . .
>
> The Commission initiated its investigation of the Passport services following a July 2001 complaint from a coalition of consumer groups led by the Electronic Privacy Information Center (EPIC).

According to the Commission's complaint, Microsoft falsely represented that:

- It employs reasonable and appropriate measures under the circumstances to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Passport Wallet services, including credit card numbers and billing information stored in Passport Wallet;
- Purchases made with Passport Wallet are generally safer or more secure than purchases made at the same site without Passport Wallet when, in fact, most consumers received identical security at those sites regardless of whether they used Passport Wallet to complete their transactions;
- Passport did not collect any personally identifiable information other than that described in its privacy policy when, in fact, Passport collected and held, for a limited time, a personally identifiable sign-in history for each user; and
- The Kids Passport program provided parents control over what information participating Websites could collect from their children.

The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years.[16]

FTC Chairmen Timothy J. Muris said at the time, "Good security is fundamental to protecting consumer privacy. Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law. Even absent known security breaches, we will not wait to act."[17]

Then in December 2004, EPIC filed a complaint with the Federal Trade Commission against databroker Choicepoint, urging the Commission to investigate the compilation and sale of personal dossiers by data brokers such as Choicepoint.[18] Based on the EPIC complaint, in 2005, the FTC charged that Choicepoint did not have reasonable procedures to screen and verify prospective businesses for lawful purposes and as a result compromised the personal financial records of more than 163,000 customers in its database. In January 2006, the FTC announced a settlement with

---

[16] Fed. Trade Comm'n, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises: Passport Single Sign-In, Passport "Wallet," and Kids Passport Named in Complaint Allegations,* Press Release, (Aug. 8, 2002), *https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy.*

[17] *Id.*

[18] EPIC, ChoicePoint, *https://www.epic.org/privacy/choicepoint/*

Choicepoint, requiring the company to pay $10 million in civil penalties and provide $5 millions for consumer redress. EPIC's Choicepoint complaint produced the largest civil fine at the time in the history of the FTC.[19]

The Microsoft order led to user-centric identity scheme that, if broadly adopted, could have done much to preserve the original open, decentralized structure of the Internet. The Choicepoint order led to significant reforms in the data broker industry. And it is worth noting that both investigations were successfully pursued with Republican chairmen in charge of the Federal agency and both actions were based on unanimous decisions by all of the Commissioners.

The Facebook complaint should have produced an outcome even more consequential than the complaints concerning Microsoft and Choicepoint. In 2011, the FTC, based the materials we provided in 2009 and 2010, confirmed our findings and recommendations. In some areas, the FTC even went further. The FTC issued a Preliminary Order against Facebook in 2011 and then a Final Order in 2012.[20] In the press release accompanying the settlement, the FTC stated that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[21]

According to the FTC, under the proposed settlement Facebook is:

- "barred from making misrepresentations about the privacy or security of consumers' personal information;"
- "required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;"
- "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;"
- "required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and"
- "required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected."[22]

The reporting requirements are set out in more detail in the text of the Final Order. According to the Final Order:

> [The] Respondent [Facebook] shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:
>
> A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
>
> B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.
>
> C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and reg-

---

[19] Fed. Trade Comm'n., *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress: At Least 800 Cases of Identity Theft Arose From Company's Data Breach* (Jan. 26, 2006), *https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.*

[20] Facebook Consent Order.

[21] Fed. Trade Comm'n., *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises,* Press Release, (Nov. 29, 2011), *https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.*

[22] *Id.*

ular testing or monitoring of the effectiveness of those controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.[23]

Moreover, the Final Order stated:

Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.[24]

EPIC expressed support for the Consent Order but also believed it could be improved.[25] In response to the FTC's request for public comments on the proposed order we wrote:

EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the Commission. Consistent with this earlier determination, to protect the interests of Facebook users, and in light of recent changes in the company's business practices, EPIC urges the Commission to require Facebook to:

---

[23] Facebook Consent Order.

[24] *Id.* at 6–7.

[25] Comments of EPIC, *In the Matter of Facebook, Inc.*, FTC File No. 092 3184, (Dec. 27, 2011), *https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.*

- Restore the privacy settings that users had in 2009, before the unfair and deceptive practices addressed by the Complaint began;
- Allow users to access all of the data that Facebook keeps about them;
- Cease creating facial recognition profiles without users' affirmative consent;
- Make Facebook's privacy audits publicly available to the greatest extent possible;
- Cease secret post-log out tracking of users across websites.

At the time, the FTC settlement with Facebook was widely viewed as a major step forward for the protection of consumer privacy in the United States. The Chairman of the FTC stated, "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not." Mark Zuckerberg said at the time of the Consent Order that the company had made "a bunch of mistakes."[26] The FTC Chair called Mr. Zuckerberg's post a "good sign" and said, "He admits mistakes. That can only be good for consumers."[27]

Commissioners and staff of the FTC later testified before Congress, citing the Facebook Consent Order as a major accomplishment for the Commission.[28] And U.S. policymakers held out the FTC's work in discussions with trading partners for the proposition that the U.S. could provide privacy protections to those users of U.S.-based services. For example, former FTC Chairwoman wrote this to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission:

> As part of its privacy and security enforcement program, the FTC has also sought to protect EU consumers by bringing enforcement actions that involved Safe Harbor violations. . . . Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new Privacy Shield Framework. . . . Consequently, these FTC orders

---

[26] Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook,* N.Y. Times, at B1 (Nov. 29, 2011), *https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html.* There was also a "lengthy blog post" from Mr. Zuckerberg in the N.Y. Times article but the link no longer goes to Mr. Zuckerberg's original post. Mr. Zuckerberg's post in 2009 that established the Bill of Rights and Responsibilities for the site has also disappeared. This is the original link: *http://blog.facebook.com/blog.php?post=54746167130.*

[27] Julianne Pepitone, *Facebook settles FTC charges over 2009 privacy breaches,* CNN Money (Nov. 29, 2011), *http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm.*

[28] According to the statement of the FTC Commissioners who testified before the Senate Commerce Committee in 2012:

Similar to the Google order, the Commission's consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes that information.

The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm on Commerce, Science and Transportation, at 18, 112th Cong. (May 9, 2012) (statement of Fed. Trade Comm'n.), https://www.ftc.gov/sites/default/files/documents/public_*statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf; see also, The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (May 19, 2012)* (statement of Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n) ("We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than one billion users worldwide. As a Commissioner, I will urge continuation of this strong enforcement record."), *https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120509privacytestimony.pdf.*

help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.[29]

Yet the Federal Trade Commission never charged Facebook with a single violation of the 2011 Consent Order.

Facebook's Repeated Disclosures of Personal Information to Third Parties

On March 16, 2018, Facebook admitted the unlawful transfer of 50 million user profiles to the data mining firm Cambridge Analytica, which harvested the data obtained without consent to influence the 2016 U.S. presidential election.[30] Relying on the data provided by Facebook, Cambridge Analytica was able to collect the private information of approximately 270,000 users and their extensive friend networks under false pretenses as a research-driven application.[31] Facebook now says that the number of users who had their data unlawfully harvested was actually closer to 87 million.[32]

But the Cambridge Analytica breach, it turns out, is only the beginning. In the weeks since Facebook CEO Marc Zuckerberg told this Committee "[e]very piece of content that you share on Facebook you own. You have complete control over who sees it and how you share it," we have learned that that is far from the truth. On June 3, 2018, the New York Times reported that Facebook has "data-sharing partnerships" with at least 60 device makers.[33] "Data-sharing partnership" is a nice way of saying that Facebook was giving your personal information, and the personal information of all your friends, to companies like Apple, Amazon, BlackBerry,

Microsoft and Samsung for the last decade. The New York Times found that "[s]ome device makers could retrieve personal information even from users' friends who believed they had barred any sharing."[34] Facebook had similar agreements with Chinese phone manufacturers, including Huawei, a company that American intelligence officials have called a national security threat.[35] These partnerships predated the 2011 FTC Consent Order and are reportedly still in effect.

Both the Cambridge Analytica breach and the partnerships with device makers are in clear violation of the 2011 Consent Order, which states that Facebook "shall not misrepresent in any manner, expressly or by implication . . . the extent to which [Facebook] makes or has made covered information accessible to third parties; and the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides."[36] Part II of the proposed order required Facebook to "give its users a *clear and prominent notice* and *obtain their affirmative express consent* before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings."[37] Part IV "requires Facebook to *establish and maintain a comprehensive privacy program* that is reasonably designed to: (1) Address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook's size and complexity, the nature and scope of its activities, and the sensitivity of covered information."[38]

---

[29] Letter from FTC Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 4–5 (Jul. 7, 2016), *https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v*

[30] Press Release, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook* (Mar. 16, 2018), *https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/*.

[31] *Id.*

[32] Cecilia Kang and Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users,* N.Y. Times, (Apr. 4, 2018), *https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.*

[33] Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, *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.*

[34] *Id.*

[35] Michael LaForgia and Gabriel J.X. Dance, *Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence,* N.Y. Times (June 5, 2018), *https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html.*

[36] Federal Trade Commission, *Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment,* 76 Fed. Reg. 75883 (Dec. 5, 2011), *https://www.ftc.gov/sites/default/files/documents/federal_register_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfrn.pdf.*

[37] *Id.* (emphasis added).

[38] *Id.* (emphasis added).

Oversight of the Federal Trade Commission and Facebook Compliance with the 2011 Consent Order

Several former FTC commissioners and former FTC staff members have recently suggested that the FTC needs more authority to protect American consumers. At least with regard to enforcement of its current legal authority, we strongly disagree. The FTC could have done far more than it did.

On March 20, 2018, EPIC submitted a request to the FTC under the Freedom of Information Act for the 2013, 2015, and 2017 Facebook Assessments, as well as all records concerning the person(s) approved by the FTC to undertake the Facebook Assessments; and all records of communications between the FTC and Facebook regarding the Facebook Assessments. In 2013, EPIC received redacted version of Facebook's initial compliance report and first independent assessment after a similar FOIA request.[39] Cambridge Analytica engaged in the illicit collection of Facebook user data from 2014 to 2016, encompassed by the requested reporting period of the assessments.

EPIC's FOIA request drew attention to a version of the 2017 report available at the FTC website.[40] The 2017 Facebook Assessment, prepared by PwC, stated that "Facebook's privacy controls were operating with sufficient effectiveness" to protect the privacy of users.[41] This assessment was prepared *after* Cambridge Analytica harvested the personal data of 87 million Facebook users. The report available online is heavily redacted. EPIC is suing now for the release of unredacted report.

We will keep both Subcommittee informed of the progress of EPIC's FOIA request for the FTC reports on Facebook compliance. We also urge the Subcommittee to pursue the public release of these documents. They will provide for you a fuller pictures of the FTC's lack of response to the looming privacy crisis in America.

Recommendations

There is a lot of work ahead to safeguard the personal data of Americans. Here are a few preliminary recommendations:

- *Improve oversight of the Federal Trade Commission.* The FTC has failed to protect the privacy interests of American consumer and the Commission's inaction contributed directly to the Cambridge Analytica breach, and possibly the Brexit vote and the outcome of the 2016 Presidential election. Oversight of the Commission's failure to enforce the 2011 consent order is critical, particularly for the Senate Commerce Committee which also bears some responsibility for this outcome.
- *Update U.S. privacy laws.* It goes without saying (though obviously it still needs to be said) that U.S. privacy law is out of date. There has always been a gap between changes in technology and business practices and the development of new privacy protections. But the gap today in the United States is the greatest at any time since the emergence of modern privacy law in the 1960s. The current approach is also unnecessarily inefficient, complex, and ineffective. And many of the current proposals, *e.g.,* better privacy notices, would do little to protect privacy or address the problems arising from Cambridge Analytica debacle.
- *Establish a Federal privacy agency in the United States.* The U.S. is one of the few developed countries in the world without a data protection agency. The practical consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber attack by criminals and foreign adversaries. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security.

Conclusion

The 2011 Consent Order against Facebook was issued to protect the privacy of user data. If the FTC had done its job and enforced the Order, the transfer of 87 million user records to Cambridge Analytica could have been avoided.

---

[39] Facebook Initial Compliance Report (submitted to FTC on Nov. 13, 2012), *http://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf;* Facebook Initial Independent Assessment (submitted to FTC on Apr. 22, 2013), *http://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf.*

[40] PWC, *Independent Assessor's Report on Facebook's Privacy Program* (Feb. 11, 2017), *https://epic.org/foia/ftc/facebook/EPIC-18-03-20-FTC-FOIA-20180418-FB-Assessment-2017.pdf.*

[41] *Id.* at 4.

After this week's hearing, the Subcommittee should ask current and former FTC Commissioners and key staff, "why didn't you enforce the 2011 Consent Order against Facebook and prevent this mess?" [42]

We ask that this letter be submitted into the hearing record. EPIC looks forward to working with the Subcommittee.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Enid Zhou*
Enid Zhou
EPIC Open Government Fellow

/s/ *Sunny Kang*
Sunny Kang
EPIC International Consumer Counsel

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Counsel

Attachment

EPIC, *et al. In the Matter of Facebook, Inc: Complaint, Request for Investigation, Injunction, and Other Relief,* Before the Federal Trade Commission, Washington, DC (Dec. 17, 2009) (29 pages, 119 numbered paragraphs) (signatories include The Electronic Privacy Information Center, The American Library Association, The Center for Digital Democracy, The Consumer Federation of America, Patient Privacy Rights, Privacy Activism, Privacy Rights Now Coalition, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation).

Senator MORAN. The hearing record will remain open for two weeks. During this time, Senators are asked to submit any questions for the record. Upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible, but no later than July 19, 2018. You all have been very gracious and kind in indicating that you have significant willingness to follow up with us.

This concludes the hearing. And again, thank the witnesses. The hearing is now adjourned.

[Whereupon, at 4:50 p.m., the hearing was adjourned.]

[42] *See* Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess,* Techonomy (Mar. 22, 2018), *https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/*.

A P P E N D I X

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Thank you, Mr. Chairman, for holding this hearing.

In April, the Commerce Committee held a hearing with the Judiciary Committee in the wake of press reports that Cambridge Analytica had used Facebook data to build psychological profiles of users and target them with political propaganda. Since then, we have also learned from the *Associated Press* that former employees of Cambridge Analtyica are working with a new company doing work for numerous political campaigns.

Furthermore, we have learned from the *New York Times* that, for the past decade, Facebook has forged business partnerships with at least sixty electronics manufacturers that had access to Facebook's proprietary interface or A.P.I.

As a result, these companies had access to large amounts of users' personal information. One of Facebook's partnerships is with the Chinese device manufacturer, WAH–WAY—a company known to have ties to the Chinese government and may pose a threat to national security.

I am troubled that these agreements never came up during our April hearing. Facebook CEO Mark Zuckerberg failed to utter a single word about them when he told members that his company ended its policy allowing app developers to access friends' data. And, in this senator's humble opinion, he should have disclosed this and because of that he should probably return before the committee to answer additional questions.

Meantime, in response to the Times' reporting, Chairman Thune and I did send a letter to Mr. Zuckerberg asking numerous questions about the nature of these business partnerships and whether consumers and the FTC were aware of their existence.

This latest reporting by the *New York Times* reveals yet another dimension to the Facebook business model that raises questions about consumer privacy and information security.

Facebook asserts that these business partnerships and agreements were perfectly legitimate and necessary to enable Facebook to work on mobile devices during the early days of the mobile market. This might very well be true, but it sure looks like they are compromising user privacy without their notice and/or consent.

At today's hearing, I hope to hear from our witnesses about how Facebook handles user information in general.

Thank you, Mr. Chairman.

ASSOCIATION FOR COMPUTING MACHINERY (ACM)
U.S. TECHNOLOGY POLICY COMMITTEE (USACM)
Washington, DC, July 2, 2018

Hon. JERRY MORAN, Chair,
United States Senate,
Comm. on Commerce, Science, and Transportation,
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security,
Washington, DC.

Hon. RICHARD BLUMENTHAL, Ranking Member,
United States Senate,
Comm. on Commerce, Science, and Transportation,
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security,
Washington, DC.

Re: Recommendations and Call for Action to Address Data Privacy *Risks and Harms Revealed by Facebook/Cambridge Analytica Inquiries*

Dear Chairman Moran and Ranking Member Blumenthal:

ACM, the Association for Computing Machinery, is the largest and longest-established association of computing professionals in the world, representing approximately 50,000 individuals in the United States and 100,000 globally. USACM is the organization's U.S. Technology Policy Committee, charged by ACM with providing policy and law makers throughout government with timely, substantive and apolitical input on computing technology and the legal and social issues to which it gives rise.

We do so today in the form of the attached statement respectfully and timely submitted for the record of the Subcommittee's hearing on "*Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks,"* conducted on June 19. In our attached letter of April 9 (entered into the record of the full Committee's joint hearing with the Judiciary Committee of April 10 and Appendix A to the attached Statement),* we urged "Congress to comprehensively revisit whether the public interest can adequately be protected by current legal definitions of consent, the present scope of Federal enforcement authority, and existing penalties for breach of the public's privacy and trust on a massive scale."

In candor, we believe that early recommendation to have been too conservative to fully serve the public interest. USACM thus now concludes and recommends in the attached statement that "[g]iven the significance of the privacy and ethical shortcomings" brought to light by the joint Committees' and Subcommittee's inquiries, "now is the time for Congress to act to protect the public interest and the integrity of the democratic process by adopting comprehensive and effective personal privacy protection legislation."

On behalf of USACM, thank you and the Subcommittee for undertaking a full and public exploration of the causes, scope, consequences and implications of the enormous breaches of privacy and public trust resulting from Facebook's and outside parties' use and misuse of vast amounts of Facebook users' and millions of others' data. Recognizing that these issues and their consequences extend far beyond any single online platform or channel, and that a robust understanding of relevant technology is essential to effectively legislating, the expert members of USACM and ACM—many of them true luminaries in computer science, engineering and associated disciplines—stand ready to assist your work in any way that we can.

Thank you for your consideration of both the technical and ethical recommendations detailed in the attached record statement, and for the Subcommittee's ongoing commitment to the public's protection. To arrange a technical briefing, or should you have any other questions, please contact ACM's Director of Global Public Policy, Adam Eisgrau, at 202–580–6555 or eisgrau@acm.org.

Sincerely,

STUART SHAPIRO,
Chair.

CC: Hon. John Thune, Chairman
Senate Committee on Commerce, Science, and Transportation
Hon. Bill Nelson, Ranking Member
Senate Committee on Commerce, Science, and Transportation

Attachments
Statement for the Record of "Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks," June 19, 2018

* USACM's April 9 letter bore its prior name, "U.S. Public Policy Council," which changed to the above on July 1.

STATEMENT OF THE ASSOCIATION FOR COMPUTING MACHINERY,
U.S. TECHNOLOGY POLICY COMMITTEE

EXECUTIVE SUMMARY

ACM, the Association for Computing Machinery, is the world's largest and longest-established association of computing professionals representing approximately 50,000 individuals in the United States and 100,000 worldwide. ACM's U.S. Technology Policy Committee (USACM) is charged with providing policy and law makers throughout government with timely, substantive and apolitical input on computing technologies and the legal and social issues to which they give rise.

USACM commends the Committee and Subcommittee for delving deeply into the causes, conse-quences and implications of the Facebook/Cambridge Analytica data breaches and related failures to protect the information and privacy of millions and the integrity of democratic processes. This statement offers a synthesis of the circumstances of this series of choices and results. In addition, without endorsing any specific statutory proposal, it also makes a series of recommendations for how legislative and regulatory responses might be crafted to address the most serious technical and ethical issues raised by the Facebook/Cambridge Analytica matter, with broader applicability to all digital environments.

Fundamentally, USACM recommends that Congress craft and adopt comprehensive, risk-based privacy protections that achieve nine critical and distinct objectives. Those objectives, and USACM's conceptual recommendations for how regulators and enterprises can meet them, are:

1. Limit collection and minimize retention of personal data [1]

- Collect and retain only personal data essential for the collector to provide its service or product.
- Collect data only from active account holders (or members).
- Mitigate the risk of privacy breaches by minimizing the identifiability of data collected or retained, regardless of how minimal or briefly held.

2. Clarify and simplify user consent processes and maximize user control of data

- Provide individuals with easily understood and centrally accessible consent options specific to the type, scope, and purpose of data use to assure users' meaningful and fully informed consent.
- Allow users to easily limit the collection, creation, retention, sharing, and transfer of personal data.
- Prevent personal data obtained for one purpose from being used or made available for other purposes without fully informed consent.
- Encourage research into and the development of smart, automated privacy agents to infer privacy preferences, establish smart defaults, and scaffold decisions about consent and disclosure.

3. Simplify data sharing policies and assure transparency in data flows

- Provide individuals, prior to data collection and creation, with clear and concise information about: how and by whom their personal data is collected; how it will be used; how long it will be retained; to whom and why it may be disclosed; and how they may access, modify, and delete their data.
- Maintain an auditable list of third parties with whom each person's data has been shared, including what was shared and for what purpose(s).
- Incorporate visualization tools into platform designs to enhance users' understanding of how their data are being used.

4. Clearly define and disclose data ownership terms and attendant rights

- Clarify data ownership boundaries, including who owns data that is collected and used to support platform interoperability, platform engagement, and platform support.
- Develop binding best practices to assure transparency about data sources, so that users and authorities can determine the origin of data and bar the use of data unlawfully acquired.

[1] The term "data" is used broadly throughout this statement to encompass personal information, patterns of individual behaviors, identifying imagery, and spatial presence.

5. Adopt and enforce data security practices commensurate with risk

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
- Audit the access, use, and maintenance of personal data.
- Report data privacy breaches as quickly as possible.

6. Require clear, fair, and responsible data access, retention, and disposal policies

- Establish clear policies with fixed, publicly-stated retention periods and seek affirmative consent to retain personal data for longer periods, if needed.
- Reduce the risk of data loss by using de-identification, aggregation, encryption, and other methods to reduce the data's accessibility.
- Implement an auditable process for verifying that data has been deleted when requested, including data provided to third, fourth, and other downstream parties.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including backup data and information shared with third and other downstream parties.

7. Codify appropriate and meaningful oversight of third party developer platforms (API)

- Publish clear guidelines for app developers regarding acceptable and unacceptable uses of data.
- Require oversight, review, and enforcement of policies regarding the types of apps and uses of data that are allowed, with clear consequences for misuse.
- Ensure that the terms of service for all applications deployed on, by or through a platform are consistent with the platform's own data use policies.

8. Enable and support legitimate and appropriately overseen platform research

- Design platforms to facilitate robust research access.
- Encourage platforms to publish guidelines for researchers detailing: acceptable use of data, procedures for protecting user privacy, data retention practices, and other expectations of those conducting research on the platform.
- Allow researchers to submit evidence of approval for studies that have been reviewed by institutional review boards or other appropriate human subjects protection boards.
- Enforce consequences for conducting unauthorized research studies and/or failing to adhere to published guidelines.

9. Measure the actions and omissions of companies against all appropriate ethical standards, including ACM's Code of Ethics. The Code affirms that all computing professionals should:

- Contribute to society and to human well-being working to minimize the negative consequences of systems, and ensure their developments will be used in socially responsible ways. (ACM Code *§ 1.1*)
- Avoid harm to others, where harm includes "negative consequences" or the "undesirable loss of information or property." (ACM Code *§ 1.2*)
- Respect privacy by only using personal data for legitimate ends and without violating the rights of individuals and groups. (ACM Code *§ 1.6*)
- Consider and mitigate the possible risks of the systems they develop. (ACM Code *§ 2.5*)
- Ensure that the public good is a central concern. (ACM Code *§ 3.1*)
- Provide responsible stewardship of systems embedded in society. (ACM Code *§ 3.7*)

Given the significance and breadth of the privacy and ethical shortcomings at the core of the Cambridge Analytica matter, USACM believes that now is the time for Congress to act to protect the public interest and the integrity of the democratic process by adopting comprehensive and effective personal privacy protection legislation.

Although data[2] privacy issues create recurring challenges to a broad sector of industries, the social media context creates unique challenges. This is especially apparent in Facebook, the largest social media community in the world, the leading revenue generator in the industry, and the primary social media platform choice of Americans.[3] These challenges spring from:

1. *Scale*—Globally, there are approximately 2.2 billion Facebook, 1.5 billion YouTube, 813 million Instagram, and 330 million Twitter users of social media.[4] Among 325 million U.S. adults, 68 percent use Facebook, 73 percent use YouTube, 35 percent use Instagram, and 24 percent use Twitter, and 60–75 percent of these are daily users.[5] This creates an enormous platform for data collection and third party usage.
2. *Influence*—The network structure of social media, where individuals are directly connected to friends and indirectly to friends of friends (and their friends), creates a highly effective platform for spreading influence through information and opinions. Services designed to build and reinforce healthy social connections can also be used to manipulate and influence opinion.
3. *Social context*—Compared to the individual and transactional nature of other online environments (*e.g.,* banking, commerce, and health), social media is grounded in social interactions, relationships, and reputations. As such, decisions, behaviors, and consequences are rarely confined to the individual level.
4. *Assumptions of risks*—Connecting and sharing with friends are considered non-transactional and therefore appear to create less risk than online purchasing. Similarly, disclosures among trusted friends are considered less risky than public disclosures, and many users, regardless of their privacy settings, still consider their social media disclosures "among friends."
5. *Technical synergies* that reinforce effects create an environment that engenders problematic security and privacy practices. This includes platform architecture, data aggregation, micro-targeting algorithms, and application programming interfaces (APIs).

The unique circumstances of the Facebook-Cambridge Analytica data breach included consequences that extend beyond individual or social levels, to the disruption of national democratic processes. Data on U.S. citizens was specifically harvested by agents outside of the U.S. to develop predictive models and ads targeted at voter manipulation in the 2016 presidential election. This operation employed large-scale collection and sharing of datasets from the Facebook platform, under the guise of research. Derivative data were subsequently sold (at a price of $500,000) to a private data harvesting firm to develop profiles for targeted ad deployment. Assessments of the operation's effectiveness vary, but the very existence of the attempt to manipulate the public in this manner highlights the risks of social media data sharing.

The Cambridge Analytica incident illustrates the difficulties of monitoring and regulating data that is collected from one site (*Facebook*), analyzed at a second site (*Cambridge University*), and then sold to a third site (*Cambridge Analytica*) where it was used to influence our systems of government. Moreover, this situation was foreseeable, and specifically described in reports as early as 2010.[6] Furthermore, although Cambridge Analytica has closed its doors,[7] a new com-pany has already been created (Data Propria) that includes employees from Cambridge Analytica and alleged access to the data collected from the Facebook community and its derivatives.[8]

In other words, election interference using social media channels and data mined from social media communities was predicted, has happened, and is continuing in current campaigns today—nationally and globally. This means that democracy in the United States remains vulnerable to the type of assault committed in 2016. The

---

[2] The term "data" is used broadly throughout this statement to encompass personal information, patterns of individual behaviors, identifying imagery, and spatial presence.

[3] Smith, A., & Anderson, M. (2018, Mar 1). Social Media Use in 2018. *Pew Research Center. http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/*

[4] Statistica (2018). Social media: Statistics and facts. *Statistica: The statistics portal. https://www.statista.com/topics/1164/social-networks/*

[5] Smith, A., & Anderson, M. (2018, Mar 1). Social Media Use in 2018. *Pew Research Center.*

[6] Electronic Privacy Information Center. (2010). e-Deceptive Campaign Practices (2010). *http://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf,* p. 25

[7] Ballhaus, R., & Gross, J. (2018, May 2). Cambridge Analytica Closing Operations Following Facebook Data Controversy. *Wall Street Journal. https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140*

[8] Horwitz, J. (2018, June 15). Trump 2020 working with ex-Cambridge Analytica staffers. *AP News. https://apnews.com/96928216bdc341ada659447973a688e4*

processes to inoculate voters against this influence or manipulation remain to be established. This should not be seen as a partisan activity but one to protect democracy from those who would do it harm.

This case and its breaches of data and trust challenge fundamental principles of privacy protection that have been enumerated in statements and laws over the years, including the *Fair Information Practice Principles* first codified in the U.S. Privacy Act in 1974 [5 U.S.C. § 552a]. The case also raises questions about the ethical responsibilities of Facebook and other social media companies in their professional practice, as well as the design of platforms that advantage revenue over the protection of user privacy. We elaborate on these in the following sections.

PRIVACY

Data capture mechanisms continue to evolve. Meanwhile, threat actors seek to exploit vulnerabilities to circumvent security and improperly access personal data (*e.g.,* the 2015 OPM[9] and 2017 Equifax[10] data breaches). Given the number and magnitude of reported data breaches, the US, like the EU, is at a pivotal point, and must take a retrospective, holistic, and comprehen-sive view of data breaches. Policy makers should consider risk-based comprehensive privacy reform with broad privacy statements to maintain pace with technological advancements. Any new data privacy protections should aim to:

1. Limit collection and minimize retention of personal data

Numerous kinds of data collection within the Facebook platform exceed the scope expected by users and, in some cases, take place without the informed consent of the users. For example, data is collected about friends of friends (who were not given the opportunity to permit such data sharing), and through third-party apps. This data is then used for secondary or tertiary purposes without the knowledge or consent of users and sometimes, as in the case of Cambridge Analytica, in violation of third-party terms of agreement.

In addition, Facebook collects data on non-Facebook account holders, conducts off-platform tracking of users to support data security and platform interoperability, and accesses cookies to feed advertising delivery. Facebook also has data-sharing partnerships with more than 60 device makers, including Amazon, Apple, Microsoft, and Samsung,[11] as well as four Chinese electronics businesses, including one that has been identified as a national security threat.[12] The device-maker partnerships provide third party business associates with access to personal data of Facebook users and their friends, without explicit consent. Most of these collection activities are not transparent to users.

Recommendations:

- Collect and retain only personal data essential for the collector to provide its service or product.
- Collect data only from active account holders (or members).
- Mitigate the risk of privacy breaches by minimizing the identifiability of all data collected or retained, regardless of how minimal or briefly held.

2. Clarify and simplify user consent processes and maximize user control of data

Addressing user consent in large-scale social media contexts is admittedly complicated, and current consent practices are generally ineffective. Specifically, consent in social media environments is overbroad (blanket consent for very nuanced uses of data), and users often consent even when the risks are high,[13] or because they

---

[9] Nakashima, E. (2014, Jul 9). Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say. *Washington Post. https://www.washingtonpost.com/news/federaleye/wp/2015/07/09/hack-of-security-clearance-system-affected-21–5-million-people-federal-authoritiessay/?utm_term=.305e75d6db3d*

[10] Matthews, L. (2017, Sep 7). Equifax Data Breach Impacts 143 Million Americans. *Forbes. https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-millionamericans/#5dd854a4356f*

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

[12] LaForgia, M. & Dance, G.J.X. (2018, June 5). Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence. N.Y. Times. *https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html?smprod=nytcore-ipad&smid=nytcore-ipad-share*

[13] Alessandro Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy, Jan./Feb.,* 26–29.

fear a loss of functionality or missing out of social engagement.[14] Consent is also not transparent, because data is often used in multiple ways beyond the original collection purpose. Consent needs to be meaningful, granular, and an opt-in norm. These terms are described below:

- *Meaningful* consent acknowledges the complexity of privacy decision-making in social computing platforms and the difficulties of consent at scale. Consent in social media environments extends beyond individual decisions, and also considers relationships, organizational commitments and the social controls (laws, policies, and codes of conduct) in which an individual is embedded.[15]
- *Granular* consent means that disclosure decisions are specific and based upon details about the type of information, audience, communication channel, and intended use for the data. Such consent is transparent so that users understand how data will be used and who will see and use it. Granular consent should be applied to limit functionality loss when opting not to share certain data.
- Finally, a significant body of research indicates that *opt-in* defaults, where data sharing will not occur unless the user explicitly grants permission, are much more likely to align with user preferences than opt-out defaults.[16] [17] [18]

User consent policies must also address third-party data sharing and data provenance. In the Facebook/Cambridge Analytica case, data was collected by a research-based "personality game."[19] Individuals may have read their privacy policy and been comfortable with data collection. But when their data is shared with third and fourth parties, data ownership and control of the data is often lost. Worse, in this case, friends of friends who did not provide consent for data collections, had their data released to a third party and manifest itself in unknown downstream locations. In general, U.S. laws do not provide protection for data that is reused and re-disclosed (except in sectoral law, *e.g.,* HIPAA and GLBA). Thus, once information is leaked and in the possession of a third party, the person involved will not know who has the data, if it is correct or current, and has no control over it.

Recommendations:

- Provide individuals with easily understood and centrally accessible consent options specific to the type, scope, and purpose of use to assure meaningful and fully informed consent.
- Allow users to easily limit the collection, creation, retention, sharing, and transfer of personal data.
- Prevent personal data obtained for one purpose from being used or made available for other purposes without informed consent.
- Encourage research into and the development of smart, automated privacy agents (*e.g.,* P3P[20] was an early attempt) to infer privacy preferences, establish smart defaults,[21] and scaffold decisions about consent and disclosure.

3. Simplify data sharing policies and assure transparency in data flows

Facebook has failed to provide clear and conspicuous notice of its data collection practices (*e.g.,* friend of friend data capture, and off-platform data collection) and new uses of the data. Indivi-duals are not given clear information regarding what data is being collected. Furthermore, Facebook has shared repurposed data with third parties without proper consent. Collection of data under the guise of social

---

[14] Przybylski, A., Murayama, K., DeHaan, C., & Gladwell, V. (2013). Motivational, emotional and behavioural correlates of fear of missing out. *Computers in Human Behaviour, 29,* 1841–1848.

[15] Schwartz, P. M. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review, 52,* 1609–1612.

[16] Cranor, L. F., Guduru, P. & Arjula, M. (2006). User interfaces for privacy agents. *ACM Trans. Comput.-Human Interaction, 13,* 2 (June 2006), 135–178.

[17] Cranor, L. F. (2012). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications and High Technology Law, 10,* 273.

[18] McQuinn, A. (2017, October 6). The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules. *https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules*

[19] Kogan, A. (2018, June 19). *The Threat of Data Theft to American Consumers.* Testimony on behalf of USACM before the Senate Comm. on Commerce, Science and Transportation, S. Comm. on Consumer Protection, Product Safety, Insurance, and Data Security. Washington, DC. *https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=484EFD3A-63F9-40BA-B212-12311F3DE7ED*

[20] Cranor, L. F., Guduru, P. & Arjula, M. (2006). User interfaces for privacy agents. *ACM Trans. Comput.-Human Interaction, 13,* 135–178.

[21] Knijnenburg, B.P. (2015). *A User-Tailored Approach to Privacy Decision Support.* PhD dissertation, University of California Irvine.

games (*e.g.,* personality tests) obscures and violates transparency of data use. For example, apps that entice engagement but come attached with obscured ("back door") consent to allow data sharing, mask the true nature of platform engagement and data collection. Facebook also has device partnerships with over 60 device firms, and provides access to user data with these partners, including international firms with less secure data protection laws.[22]

Recommendations:

- Provide individuals, prior to data collection and creation, with clear and concise information about how and by whom their personal data is being collected, how it will be used, how long it will be retained, to whom and why it may be disclosed, and how they may access, modify, and delete their own data.
- Maintain an auditable list of third parties with whom each person's data has been shared, including what was shared and for what purpose(s).
- Incorporate visualization tools into platform designs to enhance users' understanding of how their data are being used.[23]

4. Clearly define and disclose data ownership terms and attendant rights

It is critical to clarify differences in data types and how they affect the concept of ownership, and its underlying rights. During the April congressional hearings, Mark Zuckerberg provided numerous assurances that every Facebook user owns and controls their data, stating: *"This is the most important principle for Facebook. Every piece of content that you share on Facebook you own, and you have complete control over who sees it and how you share it."* [24]

But Facebook's "complete control" policy protects data that *users contribute* in postings and comments; the protections do not extend to data not explicitly provided by users, but instead derived from user behavior (*i.e., derivative data),* such as liking behavior, friending patterns, metadata on content shared, and devices used. Furthermore, vast troves of data are collected from third party partners, app developers, and data brokers, who provide information about activities off Facebook, and are then aggregated with user-contributed data. Individuals do not have ownership, or complete control, over these data. (For an extensive list of data collected, see Mr. Zuckerberg's responses to the Senate Judiciary Committee.) [25]

In spite of its ongoing rhetoric of building social communities, by its own admission,[26] at its core Facebook is a platform to collect, generate, and commodify user data. Once engaged, individuals have relatively little control over how their data is used.

Recommendations:

- Clarify data ownership boundaries, including who owns data that is collected and used to support platform interoperability, platform engagement, and platform support.
- Develop binding best practices to assure transparency about data sources, so that users and authorities can determine the origin of data and bar the use of data unlawfully acquired.

5. Adopt and enforce data security practices commensurate with the risk

Facebook relinquishes oversight after sharing data with third parties, and therefore does not audit or track uses beyond the original intent for which it was captured and shared. Nor is it alone in these practices. Considering the extensive and demonstrable risk presented by the accumulation of data (which is uniquely large-scale and detailed), little has been done to institute appropriate provisions to protect personal data. This should include risk assessments, processes to ensure that data is accessed according to Facebook policy, and proper auditing to track who is accessing what.

---

[22] Dance, G.I.X., Confessore, N., & LaForgia, M. (2018, June 3). *Facebook Gave Device Makers Deep Access to Data on Users and Friends,* N.Y. Times.

[23] Caine, K., Kisselburgh, L.G., & Lareau, L. (2011). Audience visualization influences online social network disclosure decisions. *Proc. of the 2011 Conference on Human Factors in Computing Systems,* 1663–1668.

[24] *Facebook, Social Media Privacy, and The Use and Abuse of Data: Joint Hearing Before the* S. *Comm. On Commerce. Sci., & Transp. and the* S. *Comm. on the Judiciary* (20 18) (statement of Mark Zuckerberg, Facebook).

[25] Facebook (2018, June). Responses to Judiciary Committee April 10, 2018 Hearing "*Facebook, Social Media Privacy, and the Use and Abuse of Data"* (p. 160–162).

[26] ibid (p. 155)

Recommendations:

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
- Audit the access, use, and maintenance of personal data.
- Report data privacy breaches as quickly as possible.

6. Require clear, fair and responsible data access, retention, and disposal policies

The means by which users can expunge their Facebook data are not intuitive, and requesting that one's data be deleted may not actually result in expunged data. For example, it is difficult for users to remove underlying, internal data that is associated with their accounts, even when their account is deleted. Additionally, in the case of Cambridge Analytica, while Facebook assured users that data had been erased, they lacked an oversight process to ensure that data stored by the third and fourth parties (*e.g.,* Cambridge University and Cambridge Analytica) was removed.

Recommendations:

- Establish clear policies with fixed, publicly stated retention periods and seek individuals' affirmative consent to retain their data for longer periods if desired by the collector.
- Reduce the risk of data loss by reducing the accessibility of data through de-identification, aggregation, encryption, and other methods.
- Implement an auditable process for validating the destruction of data when requested, including data provided to third, fourth, and other downstream parties.
- Store personal data only for as long as needed to serve the stated purpose for its initial collection.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including backup data and information shared with third parties.

7. Codify appropriate and meaningful oversight of third party developer platforms

Facebook's and others' application programming interface (API) developer platforms have been the source of many privacy breaches, allowed wide access to user data, and are subject to data use policies that often go unenforced. In 2017, for example, Facebook alone identified 370,000 apps that were in violation of its data use policy.[27] API platforms provide access to personal data to a variety of third parties, including app developers, advertisers, and researchers. However, the processes to regulate and audit anticipated use of personal data are not well enforced. Furthermore, by its own admission, the supplemental terms of service accompanying apps delivered in the Facebook platform are not reviewed.

This scenario has led to extensive background data scraping, and circumvented both user consent and data use oversight, and Cambridge Analytica was just one instance. API platform oversight must hold accountable all developers.

Recommendations:

- Publish clear guidelines for types of behavior that are acceptable and unacceptable for Facebook apps.
- Require oversight, review, and enforcement of policies regarding the types of apps and the uses of data that are allowed, with clear consequences for misuse.
- Ensure that the terms of service for all applications deployed are consistent with host data use policies.

8. Enable and support legitimate research when evaluated by qualified review boards

The rich user interactions and social dynamics of Facebook's and others' vast social networks represent a trove of opportunities for scientists interested in studying social dynamics and other related topics. Researchers are trained in, and ethically obligated to comply with, well-established regulatory frameworks that protect human participants in research studies. Facebook should both facilitate responsible

[27] Ibid (p. 217)

research while working to ensure that the privacy of Facebook users is fully protected.[28] [29]

Recommendations:

- Design platforms to facilitate robust research access.
- Encourage platforms to publish guidelines for researchers detailing: acceptable use of data, procedures for protecting user privacy, data retention practices, and other expectations of those conducting research on the platform.
- Allow researchers to submit evidence of approval for studies that have been reviewed by institutional review boards or other appropriate human subjects protection boards.
- Enforce consequences for conducting unauthorized research studies and/or failing to adhere to published guidelines.

ETHICS

In addition to longstanding issues of privacy protection for user data in social media contexts, the Facebook/CA case raises many issues surrounding professional and organizational ethics. We suggest that Facebook, through repeated violations of privacy rights and insufficient concern for the consequences of such violations, has demonstrated a fundamental lack of ethical responsibility to its community and our larger society. Their actions, and their omissions, must be measured against appropriate ethical standards.

ACM, the world's longest-established and largest computing professional society, has a longstanding *Code of Ethics and Professional Conduct* [30] that holds computing professionals and organizations to standards of responsibility and ethical practice. Specifically, the first principle of the Code states that:

> *"An essential aim of computing professionals is to minimize negative consequences of computing . . . and consider whether the results of their efforts . . . will be used in socially responsible ways."*(§ 1.1)

Fundamentally, Facebook (and other social media platforms) are designed to maximize user engagement and advertising revenue. Platforms for social engagement are based on trust and community and by their nature reduce concerns about privacy when one believes sharing is limited to friends. Users believe privacy policies protect sharing with friends.[31] [32] Yet, in spite of years of rhetoric to the contrary,[33] [34] the balance of care has minimized concerns of user privacy. While spokespersons for Facebook repeatedly have apologized for privacy breaches,[35] [36] [37] there has been no indication that Facebook will make fundamental changes to platform

---

[28] Feamster, N. (2018, Apr 10). Freedom to Tinker: Is It Time for a Data Sharing Clearinghouse for Internet Researchers? *Center for Information Technology Policy,* Princeton University. *https://freedom-to-tinker.com/2018/04/10/is-it-time-for-an-data-sharing-clearinghouse-for-internet-researchers/*

[29] Smee, B. (2018, Apr 25). Facebook's data changes will hamper research and oversight, academics warn. *The Guardian. https://www.theguardian.com/technology/2018/apr/25/facebooks-data-changes-will-hamper-research-and-oversight-academics-warn?CMP=share_btn_link*

[30] ACM (2018). *Code of Ethics and Professional Conduct. https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct*

[31] Wisniewski, P., Xu, H., Lipford, H.R., & Bello-Ogunu, E. (2015). Facebook Apps and Tagging: The Trade-off between Personal Privacy and Engaging with Friends. *J. of the Assoc. of Info Sci and Tech, 66* (9), 1883–96.

[32] Xu, H., Dinev, T., Smith, H.J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *J. of the Assoc. for Info Systems, 12*(12), 798– 824.

[33] Hoffmann, AL, Proferes, N., & Zimmer, M. (2016). "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society, 20,* 199–218.

[34] Zimmer, M. (2014, Feb 3). Mark Zuckerberg's theory of privacy. *Wash. Post. http://wapo.st/1gHIpbl?tid=ss_mail&utm_term=.7137dd0e1d99.*

[35] *Facebook, Social Media Privacy, and The Use and Abuse of Data.* Joint Hearing Before the S. Comm. on Commerce. Sci., & Transp. and the S. Comm. on the Judiciary, (20 18) (statement of Mark Zuckerberg, Facebook).

[36] Frenkel, S. (2018, May 22). Mark Zuckerberg to Apologize Again, This Time to European Parliament. *N.Y. Times. https://www.nytimes.com/2018/05/22/technology/mark-zuckerberg-apologize-european-parliament.html*

[37] Seetharaman, D. (2018, Mar 21). After Days of Silence, Facebook's Mark Zuckerberg Admits to "Mistakes" with User Data. *Wall Street Journal. https://www.wsj.com/articles/after-days-of-silence-mark-zuckerberg-to-publicly-address-facebooks-user-data-uproar-1521659989*

design to make privacy protections inherent rather than wholly dependent upon users.

In addition, Facebook's executives have repeatedly stated that they failed to recognize the potential misuse of data in their social community—a community of over 2 billion people, used by 68 percent of American adults. Ultimately, they abdicated what USACM and ACM's Code of Ethics consider their *heightened* responsibility to administer a platform that was deeply integrated into the fabric of 21st-century society, and neglected an appropriate standard of care for the members of its community and broader society.[38]

Furthermore, in the case of Cambridge Analytica, despite knowledge that data was being and had been misused, until the breach was publicized Facebook did not notify users and took few actions to alleviate the damage. Specifically, Facebook failed to identify and stop errant use of their API platform for nearly two years, and did not ensure the data was destroyed and no longer used. In this regard, they failed to abide by ethical standards regarding understanding and acknowledging the risks and consequences of systems, as well as legal standards of accountability to protect consumer privacy.[39]

At the same time, there are significant unresolved issues regarding ethical research practices in social media contexts, in both federally and privately funded venues. This includes discerning whether data is considered private or public, the challenge of garnering consent in large-scale contexts, and the ethical responsibility to inform users (either before, or by debrief after) experimental manipulation is conducted. For example, there were two published research studies conducted by Facebook involving political[40] and emotional[41] manipulation that raised significant questions in the research community about ethical research standards in social media environments.

Significantly, the use of harvested data to psychologically manipulate behavior extends beyond the generation of revenue streams to support a free community of social networking,[42] and should include careful oversight. Furthermore, given the findings of research demonstrating that political manipulation in the Facebook platform can be accomplished,[43] [44] the organization had an ethical duty to review and screen targeted ads that were designed to manipulate political opinion, and clearly failed to do this in 2016.

Codes of ethical practice exist to guide the developer in the design, development, and management of systems, and to recognize the human as well as system consequences of design failure. Computer professionals and organizations must adhere to these broadly accepted norms and ethical codes:

1. *Avoid harm to others,* where harm includes negative consequences or the undesirable loss of information or property (ACM Code § 1.2): The many cases of data breaches and disclosure of personal data within Facebook and other social media platforms, as well as the use of Facebook for political manipulation of voters, has undeniably caused harm to global citizens.
2. *Respect privacy* (ACM Code § 1.6): As numerated earlier, there are fundamental, longstanding principles of privacy protection that have been ignored both in practice as well as in system design.

---

[38] While this ethical standard was only recently included (in Section 3) of the Code of Ethics, 95 percent of surveyed ACM members responding agree it is important.

[39] Federal Trade Commission (2011, Nov 29). Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises. *https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep*

[40] Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*(7415).

[41] Kramer, A.D.I., Guillory, J.E., & Hancock, J.T. (2014). Emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788–8790.

[42] Woodruff, J. (2018, Apr 5). Facebook 'made big mistakes' on protecting user data. *PBS Newshour. https://www.pbs.org/newshour/show/sheryl-sandberg-facebook-made-big-mistakes-on-protecting-user-data*

[43] Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*(7415).

[44] Electronic Privacy Information Center. (2010). e-Deceptive Campaign Practices (2010). *http://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf, p. 25*

3. *Evaluate the possible risks* of the systems they develop (ACM Code § 2.5): By their own admission,[45] Facebook executives failed to recognize, understand, and assess the risks inherent in any platform that handles information about people. Given the vast size and influence of the Facebook platform, this was fundamentally negligent.
4. *Ensure that the public good is a central concern* (ACM Code § 3.1): With 69 percent of Americans using social media, and most of them on a daily basis, these are effectively public utilities with commensurate obligations to ensure the public good.
5. *Provide responsible stewardship of systems embedded in society* (ACM Code § 3.7): The ACM Code recently was revised to add: "When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems."

CONCLUSION

US citizens enjoy an expectation of privacy when talking on standard landline telephones. Eavesdropping on another's call is prohibited by the Wiretap Act [18 U.S. Code § 2511]. Similarly, U.S. citizens have an expectation of privacy when mailing a letter, as codified by 18 U.S. Code § 1708. However, legislation has not kept pace with technological advancements. For example, these same protections for mail and telephone do not extend to electronic communications, such as e-mail, twitter feeds, or social media posts. Instead, data from these channels are captured, aggregated, correlated, shared, and sold. Processes like deep packet inspection, web beacons, and parsing e-mail content seem equally intrusive. If you call your closest relative and share that you have the flu, that conversation is protected. However, if you e-mail those same disclosures, that communication is subject to being captured, shared, and aggregated.

Certainly, businesses have legitimate reasons to collect certain kinds of data. When making an online purchase, specific information is required (such as item, cost, payment, and location) to deliver the merchandise. Consumers see value in providing these details to fulfill a transaction. However, if the purchased merchandise was for an adult product, one might be troubled to know the merchant sold those details to a background screening company, who included that information when you later applied for a new job. Clearly some data needs to be collected. At issue are: what data to collect, how long is the data retained, is it accurate and protected, what other datasets are combined with it, and with whom is this data shared.

In summary, data collection, sharing, and management practices in the U.S. have gone largely unregulated. Facebook illustrates that organizations will continue to evolve their business models, sometimes to the detriment of consumers' security and privacy. The issues are exacerbated by the constant invention of new data collection channels (*e.g.,* smart speakers, wearable fitness trackers, smart appliances). The type and amount of data being captured is unprecedented, as is the velocity of which it is shared. The ability to cross-reference seemingly disparate data to draw conclusions is alarming. Large data stores can be monetized quickly and the raw materials to create these products are not consumed when they are sold, so they can be repackaged in perpetuity.

As technological innovation continues its exponential growth, ethical platform design and professional practice and broad scalable legislation and oversight are needed. Policy and laws that were once adequate, like the Wiretap Act, do not account for the complexities of today's socio-technical systems. Businesses today have proven unable to self-police, and so legislative and regulatory action that protects consumer privacy without materially limiting innovation is essential.

Specifically, protections are needed that limit data collection, require granular consent, transparently articulate information collection and retention, prohibit reuse/re-disclosure without informed consent, introduce expiration dates for datasets that deteriorate over time, consider the ethical consequences, introduce constructs to validate that consumer safeguards are effective, and enforce these protections.

Finally, a social media platform like Facebook is a single channel. But the broader picture indi-cates that technological advancements will continue to outpace legislation and consumers' ability to understand the ramifications of the types and amount of data being captured. Recog-nizing this, niche legislation (*e.g.,* to address only so-

[45] *Facebook, Social Media Privacy, and The Use and Abuse of Data: Joint Hearing Before the S. Comm. On Commerce. Sci., & Transp. and the S. Comm. on the Judiciary* (2018) (statement of Mark Zuckerberg, Facebook).

cial media) will not adequately protect con-sumers and will be constantly chasing emerging technological advancements. Further, given the monetary incentives, businesses will continue to find loopholes, or will alter their business model to stay ahead of legislation. Even if businesses are somehow enticed to be better data stewards, the number of publicized data breaches suggests the data will continue to leak into the wild.

Given the significance and breadth of these privacy and ethical shortcomings, USACM believes that now is the time for Congress to act to protect the public interest and the integrity of the democratic process by adopting comprehensive and effective personal privacy protection legislation.*

Respectfully submitted,

STUART SHAPIRO,
Chair.

APPENDIX A

ASSOCIATION FOR COMPUTING MACHINERY (ACM) ACM
U.S. PUBLIC POLICY COUNCIL
April 9, 2018

Hon. JOHN THUNE, Chair,
United States Senate,
Comm. on Commerce, Science, and Transportation,
Washington, DC.

Hon. BILL NELSON, Ranking Member,
United States Senate,
Comm. on Commerce, Science, and Transportation,
Washington, DC.

Hon. CHARLES GRASSLEY, Chair,
United States Senate,
Committee on the Judiciary,
Washington, DC.

Hon. DIANNE FEINSTEIN, Ranking Member,
United States Senate,
Committee on the Judiciary,
Washington, DC.

Re: *Committee Consideration of Facebook Data Compromises and Related Issues*

Dear Senators Grassley, Thune, Feinstein and Nelson:

ACM, the Association for Computing Machinery, is the world's largest and oldest association of computing professionals representing approximately 50,000 individuals in the United States and 100,000 worldwide. Its U.S. Public Policy Council (USACM) is charged with providing policy and law makers throughout government with timely, substantive and apolitical input on computing technology and the legal and social issues to which it gives rise.

On behalf of USACM, thank you and the Committees for undertaking a full and public exploration of the causes, scope, consequences and implications of the enormous breaches of privacy and public trust resulting from Facebook's and outside parties' use and misuse of vast amounts of Facebook users' and millions of others' data. The technical experts we represent—including luminaries in computer science,

---

*This document is a product of the ACM U.S. Technology Policy Committee. In consultation with the colleagues noted below affiliated with ACM's Europe Technology Policy Committee (EUACM), it was prepared by the following USACM members:

Principal Authors:
Dr. Lorraine Kisselburgh, Purdue University (Chair, USACM Ethics Working Group)
Brian Dean, Secureworks (Chair, USACM Privacy Subcommittee)

Contributors:
Dr. Flo Appel, Saint Xavier University
Lillie Coney, Independent Policy Expert
Dr. Nick Feamster, Princeton University
Dr. Fabrizio Gagliardi, Barcelona Supercomputing Center (Chair, EUACM)
Dr. Simson Garfinkel, U.S. Census Bureau (Co-Chair, USACM Al & Algorithmic Transparency Committee)
Barb Helfer, Immersion Corporation
Andy Oram, O'Reilly Media
Marc Rotenberg, J.D., Electronic Privacy Information Center, Georgetown University
Dr. George Roussos, University of London
Dr. Stuart Shapiro, MITRE Corporation (Chair, USACM)

NOTE: Non-USACM affiliations noted above are provided solely for author identification purposes. They do not signify or imply the views or endorsement of any named entity other than USACM.

engineering and other computing disciplines—stand ready to lend their expertise to you and your staffs at any time as the hearing and legislative processes progress.

USACM believes that the issues raised by this incident, and the intense scrutiny now appropriately being brought to bear on it, make this a watershed moment. The issue and challenge is not merely how to address the failings of a single company, but to understand how privacy and trust in an era of big data, pervasive networks and socially embedded platforms must be addressed in order to promote the public interest broadly in our society, including specifically the integrity of our democratic institutions.

As your Committees prepare to convene, USACM offers the following broad observations grounded in our technical understanding and commitment to the highest ethical standards in our professional practice:

- It is critical to understand the full scale and consequences of how Facebook's past and present business practices or failures compromised, and may continue to undermine, users' and others' privacy and data security. It is also critical, however, to understand the technology underlying its actions and omissions so that truly effective technical and legal means may be designed to assure the protection of privacy by limiting data collec-tion and sharing, ensuring real user consent and notice, and providing full transparency and accountability to its community members. These and other fundamental principles are detailed in USACM's 2018 *Statement on the Importance of Preserving Personal Privacy* (attached);
- The actions and omissions already confirmed or publicly acknowledged to have occurred by Facebook appear to stem from systemic deficiencies in a range of processes consid-ered essential by computing professionals, including proactive risk assessment and management, as well as protecting security and privacy by design;
- Facebook's actions and omissions should be measured against all appropriate ethical standards. The first principle of ACM's long-established Code of Ethics states that, "An essential aim of computing professionals is to minimize negative consequences of computing systems. . .and ensure that the products of their efforts will be used in socially responsible ways." Adhering to broadly accepted social norms the ethical code also requires that computing professionals "avoid harm to others," where harm includes injury, negative consequences, or undesirable loss of information or property.
- The present controversy underscores that we are living in an era of mega-scale data sets and once inconceivable computational power. Consequently, the nature, scale, depth and consequences of the data, technical and ethical breaches understood to have occurred thus far in the Facebook case are unlikely to be confined to a single company, technology or industry. That argues strongly for Congress to comprehensively revisit whether the public interest can adequately be protected by current legal definitions of consent, the present scope of Federal enforcement authority, and existing penalties for breach of the public's privacy and trust on a massive scale; and
- Size and power are not the only consequential hallmarks of the new information era. Ever more complicated and multiplying synergies between technologies (such as platform architecture, data aggregation, and micro-targeting algorithms) exponentially increase the vulnerability of personal privacy. Similarly increasing complexity in the ways that social media continues to be woven into modern life amplifies the threat. Together these trends make it clear that addressing separate elements of this rapidly changing ecosystem in isolation is no longer a viable means of protecting the public interest. Rather, we urge Congress to consider new and holistic ways of conceptualizing privacy and its protection.

Thank you again for your work at this pivotal time and for formally including this corre-spondence and the attached *Statement* in the record of your upcoming hearing. USACM looks forward to assisting you and your staffs in the future. To arrange a technical briefing, or should you have any other questions, please contact ACM's Director of Global Public Policy, Adam Eisgrau, at 202–580–6555 or eisgrau@acm.org.

Sincerely,

STUART SHAPIRO,
Chair.

Attachment
cc: Members of the Senate Commerce and Judiciary Committees

ASSOCIATION FOR COMPUTING MACHINERY (ACM)
ACM U.S. PUBLIC POLICY COUNCIL (USACM)
March 1, 2018

USACM STATEMENT ON THE IMPORTANCE OF PRESERVING PERSONAL PRIVACY

USACM believes that the benefits of emerging technologies, such as Big Data and the Internet of Things, should and need not come at the expense of personal privacy. It is hoped and intended that the principles and practices set out in this Statement will provide a basis for building data privacy into modern technological systems. USACM encourages the development of innovative solutions to achieve these goals.

FOUNDATIONAL PRIVACY PRINCIPLES AND PRACTICES

Fairness

- An automated system should not produce an adverse decision about an individual without the individual's full knowledge of the factors that produced that outcome.

Transparency

- Provide individuals with clear information about how and by whom their personal data is being collected, how it will be used, how long it will be retained, to whom it may be disclosed and why, how individuals may access and modify their own data, and the process for reporting complaints or updates.
- Where feasible, provide these details prior to data collection and creation.
- Ensure that communications with individuals (*i.e.,* data subjects) are comprehensible, readable, and straightforward.

Collection Limitation and Minimization

- Collect and retain personal data only when strictly necessary to provide the service or product to which the data relates, or to achieve a legitimate societal objective.
- Minimize the identifiability of personal data by avoiding the collection of individual-level data when feasible, and taking into account the risk of correlation across data sets to re-identify individuals.

Individual Control

- In all circumstances, consent to acquisition and use of an individual's data should be meaningful and fully informed.
- Provide individuals with the ability to limit the collection, creation, retention, sharing and transfer of their personal data.
- Ensure that individuals are able to prevent personal data obtained for one purpose from being used or made available for other purposes without that person's informed consent.
- Provide individuals with the ability to access and correct their personal data.

Data Integrity and Quality

- Ensure that personal data, including back-up and copies forwarded to third parties, is sufficiently accurate, current, and complete for the purpose for which it is to be used.
- Conduct appropriate data quality assessments.

Data Security

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
- Audit access, use, and maintenance of personal data.

Data Retention and Disposal

- Establish clear policies with fixed publically stated retention periods and seek individuals' affirmative consent to retain their data for longer periods.
- Store personal data only for as long as needed to serve the stated purpose for its initial collection.
- Where feasible, de-identify personal information until properly destroyed.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including back-up data and information shared with third parties.

Privacy Enhancement

- Promote and implement techniques that minimize or eliminate the collection of personal data.
- Promote and implement techniques that ensure compliance with the best privacy practices as they evolve.

Management and Accountability

- Ensure compliance with privacy practices through appropriate mechanisms, including independent audits.
- Establish and routinely test the capability to address a privacy breach or other incident.
- Implement privacy and security training and awareness programs.

Risk Management

- Routinely assess privacy risks to individuals across the data life cycle using appropriate risk models.

APPENDIX B

ASSOCIATION FOR COMPUTING MACHINERY (ACM)
ACM U.S. PUBLIC POLICY COUNCIL (USACM)
March 1, 2018

USACM STATEMENT ON THE IMPORTANCE OF PRESERVING PERSONAL PRIVACY

USACM believes that the benefits of emerging technologies, such as Big Data and the Internet of Things, should and need not come at the expense of personal privacy. It is hoped and intended that the principles and practices set out in this Statement will provide a basis for building data privacy into modern techno—logical systems. USACM encourages the development of innovative solutions to achieve these goals.

FOUNDATIONAL PRIVACY PRINCIPLES AND PRACTICES

Fairness

- An automated system should not produce an adverse decision about an individual without the individual's full knowledge of the factors that produced that outcome.

Transparency

- Provide individuals with clear information about how and by whom their personal data is being collected, how it will be used, how long it will be retained, to whom it may be disclosed and why, how individuals may access and modify their own data, and the process for reporting complaints or updates.
- Where feasible, provide these details prior to data collection and creation.
- Ensure that communications with individuals (*i.e.,* data subjects) are comprehensible, readable, and straightforward.

Collection Limitation and Minimization

- Collect and retain personal data only when strictly necessary to provide the service or product to which the data relates, or to achieve a legitimate societal objective.
- Minimize the identifiability of personal data by avoiding the collection of individual—level data when feasible, and taking into account the risk of correlation across data sets to re—identify individuals.

Individual Control

- In all circumstances, consent to acquisition and use of an individual's data should be meaningful and fully informed.
- Provide individuals with the ability to limit the collection, creation, retention, sharing and transfer of their personal data.
- Ensure that individuals are able to prevent personal data obtained for one purpose from being used or made available for other purposes without that person's informed consent.
- Provide individuals with the ability to access and correct their personal data.

Data Integrity and Quality

- Ensure that personal data, including back—up and copies forwarded to third parties, is sufficiently accurate, current, and complete for the purpose for which it is to be used.
- Conduct appropriate data quality assessments.

Data Security

- Protect personal data against loss, misuse, unauthorized disclosure, and improper alteration.
- Audit access, use, and maintenance of personal data.

Data Retention and Disposal

- Establish clear policies with fixed publically stated retention periods and seek individuals' affirmative consent to retain their data for longer periods.
- Store personal data only for as long as needed to serve the stated purpose for its initial collection.
- Where feasible, de-identify personal information until properly destroyed.
- Implement mechanisms to promptly destroy unneeded or expired personal data, including back—up data and information shared with third parties.

Privacy Enhancement

- Promote and implement techniques that minimize or eliminate the collection of personal data.
- Promote and implement techniques that ensure compliance with the best privacy practices as they evolve.

Management and Accountability

- Ensure compliance with privacy practices through appropriate mechanisms, including independent audits.
- Establish and routinely test the capability to address a privacy breach or other incident.
- Implement privacy and security training and awareness programs.

Risk Management

- Routinely assess privacy risks to individuals across the data life cycle using appropriate risk models.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO JOHN BATTELLE

Question 1. Privacy Legislation: Across hearings and questions for the record, members of Congress have raised concerns about the data collection tactics used by Facebook that are not made clear to its users. As I stated during the hearing, I am interested in putting into place rules of the road for online privacy, taking into consideration the European General Data Protection Regulation. During the hearing Mr. Battelle and others offered support for the intent of GDPR, but expressed reservations about the implementation and unintended consequences. I look forward to any further thoughts from the panelists regarding how to implement data privacy rules in the United States.

In addition to any recommendations or comments on what types of legislation or other measures could help protect consumer privacy, what lessons and principles of the California Consumer Privacy Act and the GDPR should Congress consider in privacy legislation?

Answer. Implementation of sweeping legislation like those mentioned above is extremely onerous for small business. Instead of using that as an excuse to avoid legislation, the policy should incorporate remedies for smaller business (IE, enabling federation of resources and response/compliance, enabling trusted intermediaries).

The principle of empowering the consumer is embodied in both GDPR and CCPA. While well intentioned, neither envision how that empowerment will truly be effective in a modern digital marketplace. Take the principle of data portability. It's one thing to allow consumers to download a copy of their data from a platform or service. But for that data to drive innovation, it must be easily uploaded, in a defined, well-governed, machine-readable format, so that new kinds of services can flourish. Watch how large tech platforms chip away at CCPA and attempt to subvert that ecosystem from taking root. Consider how best to ensure that ecosystem will in fact exist. I'm not a legislative analyst, but there must be an enlightened way to encour-

age a class of data brokers (and yes, they're not all bad) who enable re-aggregation of consumer data, replete with permissions, revocation, validation, editing, and value exchange. Happy to talk more about this.

Question 2. You have written at length about the influence of Facebook and Google on the advertising and third party data market. In your experience, has Facebook driven the ad market as a sector to more invasively collect data about people? What other changes in the ad market can be attributed to the dominance of Google and Facebook?

Answer. Yes, without question, Facebook has driven what you describe in your initial question. But not for entirely negative reasons. Because Facebook has so much information on its users, larger advertisers feel at a disadvantage. This is also true of publishers who use Facebook for distribution (another important aspect of the platform, especially as it relates to speech and democratic discourse). Both advertisers and publishers wish to have a direct, one to one dialog with their customers, and should be able to do so on any platform. Facebook, however, has forced their business model into the middle of this dialog—you must purchase access to your followers and your readers. A natural response is for advertisers and publishers to build their own sophisticated databases of their customers and potential customers. This is to be expected, and if the data is managed ethically and transparently, should not be considered an evil.

As for other changes in the ad market that might be attributed to FB and GOOG, let's start with the venture funding of media startups, or advertising-dependent startups of any kind. Given the duopoly's dominance of the market, it's become extremely hard for any entrepreneur to find financing for ideas driven by an advertising revenue stream. Venture capitalists will say "Well, that's a great (idea, service, product), but no way am I going to fund a company that has to compete with Google or Facebook." This naturally encourages a downward spiral in innovation. Another major problem in ad markets is the lack of portable data and insights *between* Facebook and Google. If I'm an advertiser or publisher on Facebook, I'd like a safe, ethical, and practical way to know who has responded to my messaging on that platform, and to take that information across platforms, say to Google's YouTube or Adwords. This is currently far too hard to do, if not impossible in many cases. This also challenges innovation across the business ecosystem.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MAGGIE HASSAN TO JOHN BATTELLE

Question 1. The Internet has the potential to connect people with ideas that challenge their worldview, and early on many people were hopeful that the Internet would have just that effect. But too often we have seen that social media sites like Facebook serve instead as an echo chamber that polarizes people instead of bringing them together, showing them content that they are more likely to agree with rather than exposing them to new perspectives. Do you agree this is a problem? And should we be taking steps to address this echo chamber effect?

Answer. Yes, this filter bubble problem is well defined and I agree it's one of the major design challenges we face not only for Facebook, but for our public discourse as well. The public square, as it were, has become the domain of private companies, and private companies do not have to follow the same rules as, say, UC Berkeley must follow in its public spaces (Chancellor Carol Christ has been quite eloquent on this topic, see her interview at the NewCo Shift Forum earlier this year).

As to steps that might be taken, this is a serious question that balances a private corporation's right to conduct its business as it sees fit, and the rights and responsibilities of a public space/commons. I'd love to see those corporations adopt clear and consistent rules about speech, but they are floundering (see Mr. Zuckerberg's recent comments on Holocaust deniers, for example). I'd support a multi-stakeholder commission on this issue, including policymakers, company representatives, legal scholars, and civic leaders to address the issue.

Question 2. In your testimony you discuss the value of data. You stated that you think in some ways, QUOTE, "data is equal to—or possibly even more valuable than—monetary currency." We in Congress are seeking to figure out the value of data as well to help us understand the costs and benefits of protecting this data. Can you expand on what value you think data has, and how we should be thinking about measuring that value—both as citizens and as legislators?

Answer. Just as we had no idea the value of oil when it first came into the marketplace (it was used for lamps and for paving streets, and no one could have imagined the automobile industry), we still have not conceived of the markets, products, and services that could be enabled by free flowing and ethically sourced and

permissioned data in our society. It's literally too early to know, and therefore, too early to legislate in sweeping fashions that might limit or retard innovation. However, one thing I am certain of is that data—which is really a proxy for human understanding and innovation—is the most fundamentally valuable resource in the world. All money is simply data, when you think about it, and therefore a subset of data.

So how to measure its value? I think at this point it's impossible—we must instead treat it as an infinitely valuable resource, and carefully govern its use. I'd like to add my response to another Senator's question here, about new laws (GDPR and the California Ballot initiative) as added reference:

Implementation of sweeping legislation like those mentioned above is extremely onerous for small business. Instead of using that as an excuse to avoid legislation, the policy should incorporate remedies for smaller business (IE, enabling federation of resources and response/compliance, enabling trusted intermediaries).

The principle of empowering the consumer is embodied in both GDPR and CCPA. While well intentioned, neither envision how that empowerment will truly be effective in a modern digital marketplace. Take the principle of data portability. It's one thing to allow consumers to download a copy of their data from a platform or service. But for that data to drive innovation, it must be easily uploaded, in a defined, well-governed, machine-readable format, so that new kinds of services can flourish. Watch how large tech platforms chip away at CCPA and attempt to subvert that ecosystem from taking root. Consider how best to ensure that ecosystem will in fact exist. I'm not a legislative analyst, but there must be an enlightened way to encourage a class of data brokers (and yes, they're not all bad) who enable re-aggregation of consumer data, replete with permissions, revocation, validation, editing, and value exchange. Happy to talk more about this.

Question 3. Mark Zuckerberg has said that he sees Facebook more as a government than a traditional company. Among other things, governments need to be transparent and open about the decisions they make. Many large institutions have set up independent systems—such as offices of inspectors general or ombudsmen and ethics boards—to ensure transparency and internally check bad decisions. Facebook has none of those controls. What kinds of independent systems should companies like Facebook have to publicly examine and explain their decision-making?

Answer. OK, this one is simple. Facebook is NOT a government. If it is, I don't want to be a "citizen." I think Mr. Zuckerberg is failing to truly understand what a government truly is. If indeed Facebook wishes to become a nation state, then first it must decide what kind of nation state it wishes to be. It needs a constitution, a clear statement of rights, roles, responsibilities, and processes. None of these things exist at the moment. A terms of service does not a government make.

However, all of the ideas you mention make a ton of sense for Facebook at this juncture. I'd be supportive of them all.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO JOHN BATTELLE

Question 1. Facebook Audits: On April 4, 2018, following the public controversy over Cambridge Analytica's use of user data, Facebook announced several additional changes to its privacy policies. The changes include increased restrictions on apps' ability to gather personal data from users and also a policy of restricting an app's access to user data if that user has not used the app in the past three months. In addition, Facebook has committed to conducting a comprehensive review of all apps gathering data on Facebook, focusing particularly on apps that were permitted to collect data under previous privacy policies. Facebook will also notify any users affected by the Cambridge Analytica data leak.

What steps can the government take to ensure that there is proper oversight of these reviews and audits?

Answer. I think this is a simple answer: Make sure Facebook does what it says it will do, and make sure its response is a matter not only of public record, but also public comment. This should include a full and complete accounting of how the audit was done and the findings.

Question 2. From a technical standpoint, how effective are forensic methods at ascertaining information related to what data was transferred in these cases?

Answer. I'm not a technologist, I'm an entrepreneur, author, analyst and commentator. I'd defer to someone who has more knowledge than myself on issues of forensic data analysis.

Question 3. Technology for Consumer Protection: Are there any technological solutions being developed that can help address some of the issues of consumers' privacy being violated online?

Answer. Yes, there are many, likely too many to mention. Instead, what I'd like to highlight is the importance of the architecture of how data flows in our society. We should be creating a framework that allows data to flow ethically, securely, and with key controls around permissioning, editing, validation, revocation, and value exchange. Blockchains hold great promise here, but are still underdeveloped (but they're evolving rapidly).

Question 4. Data Retention: What should we, as legislators, should be thinking about to verify that—when Americans are told that their data has been destroyed—that deletion can actually be confirmed?

Answer. Independent third party auditing services that services such as Facebook must employ seems the most straightforward response. "Trust us" is not enough, we must trust and verify.

Question 5. Law Enforcement: During the hearing we had a brief discussion on the balance between privacy and sharing data with law enforcement.

What should companies keep in mind to ensure that they can appropriately assist in law enforcement investigations?

Answer. This is a delicate balance, as evinced in the varied responses to these kind of cases from companies like Apple, Twitter, Yahoo, and others. Valid search warrants, not fishing expeditions, should be the rule. We've got the framework for this already. The issue of how governments and law enforcement deal with encryption is unresolved. However, I fall on the side of enabling strong encryption, as I believe all citizens have the right to privacy. Lose that, and we lose democracy.

Questions 6. As lawmakers, what should we be aware of as we try to strike the right balance between privacy and safety in this area?

Answer. Democracy is open, messy, transparent, and has many failures. But it's the best system yet devised (in my humble opinion) and privacy lies at its core. That means criminals will be able to abuse its benefits. That is a tradeoff we have to accept and work around. Sure, it'd be great if law enforcement had access to all the data created by its citizens. Until it's abused, and cases of this kind of abuse by government are easy to find.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO ALEKSANDR KOGAN

Question. Sharing Facebook Data: In your testimony you state that you thought "collecting people's data like we did was completely normal, accepted, and that people whose data was being collected and transferred knew that is was regularly happening."

1. Can you explain why you believe such practices were normal? What made you believe that your relationship with Cambridge Analytica was accepted?
2. To your knowledge, were other third-party app developers similarly transferring, and potentially selling, the Facebook user data they collected? If so, can you provide examples or evidence of such practices?
3. To your knowledge, did officials at Facebook know about the existence of third-party apps that were transferring, and potentially selling, Facebook user data they collected? If so, can you provide examples or evidence of such knowledge?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO ALEKSANDR KOGAN

Question 1. Cambridge Analytica Data Collection: In prepared remarks, Professor Kogan speaks about a "myriad of allegations and claims," some which are said to be "speculation, exaggeration, or misinformation." I appreciate Dr. Kogan's willingness to set the record straight during the hearing and wish to ensure that a complete understanding is presented to the public.

Please describe all categories of data (*e.g.,* Facebook Likes, private messages, name, Facebook ID, et al) that was collected and *retained* by the GSR app throughout its operation. Which of these categories of data was provided to Cambridge Analytica and others?

Answer. *No Response Provided.*

Question 2. Please provide specific dates and names (or titles) of any involved parties related to the following milestones in the GSR and Cambridge Analytica operation:

a. When was the original Facebook data collection application created?

b. When were you initially contacted by Cambridge Analytica and by whom?

c. When did GSR sign a contract with Cambridge Analytica to collect Facebook user data, and who executed that contract for both parties?

d. When did the data collection for Cambridge Analytica begin and end?

e. When did your relationship with Cambridge Analytica end?

f. When were you first contacted by Facebook regarding the Cambridge Analytica data collection?

g. When did Facebook seek certification that the data was destroyed, and when was that certification provided?

Answer. *No Response Provided.*

Question 3. Did you ever notify Facebook or other parties about Cambridge Analytica's operations or related activities?

Answer. *No Response Provided.*

Question 4. What were the provisions of certifications you made to Facebook regarding the deletion of the data? What were the non-disclosure requirements of that agreement?

Answer. *No Response Provided.*

Question 5. WIRED has reported that in December 2014 another professor at Cambridge University wrote to its legal department to call attention to your relationship with Cambridge Analytica. Did Cambridge University or colleagues ever question the ethical or legal implications of your commercial research? Aside from suspension from Facebook, what repercussions have you faced from Facebook or Cambridge University over this matter?

Answer. *No Response Provided.*

Question 6. Please provide all of the names that the GSR app used and the time periods those names were used. Were these different iteration the same app as submitted to the Facebook platform, or separate applications?

Answer. *No Response Provided.*

Question 7. Please describe the measures taken to protect the confidentiality and privacy of the GSR app derived dataset that was kept by you, who you provided that dataset to, and how it was destroyed by you.

Answer. *No Response Provided.*

Question 8. What other clients and purposes (commercial or non-commercial) was the GSR app derived dataset used by you for?

Answer. *No Response Provided.*

Question 9. Please provide further information on the financial relationship with Cambridge Analytica. What payments were made in order to create the dataset, to whom were the payments made, what was the purpose, and what was the amount? Did you or GSR ever receive remuneration for consultation or other services from Cambridge Analytica beyond reimbursement for costs?

Answer. *No Response Provided.*

Question 10. Please describe Joseph Chancellor's role within GSR, particularly during the Cambridge Analytica work. To your knowledge, did Dr. Chancellor disclose this work to Facebook, was he aware of the nature of the relationship with Cambridge Analytica, and when did you last communicate with him?

Answer. *No Response Provided.*

Question 11. March 2018 reports suggested that some of the GSR dataset remains in circulation. Who do you believe kept a copy of the dataset?

Answer. *No Response Provided.*

Question 12. Privacy Legislation: Across hearings and questions for the record, members of Congress have raised concerns about the data collection tactics used by Facebook that are not made clear to its users. As I stated during the hearing, I am interested in putting into place rules of the road for online privacy, taking into consideration the European General Data Protection Regulation. During the hearing Mr. Battelle and others offered support for the intent of GDPR, but expressed reservations about the implementation and unintended consequences. I look forward to any further thoughts from the panelists regarding how to implement data privacy rules in the United States.

In addition to any recommendations or comments on what types of legislation or other measures could help protect consumer privacy, what lessons and principles of the California Consumer Privacy Act and the GDPR should Congress consider in privacy legislation?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO ALEKSANDR KOGAN

Question 1. You have disclosed that you received funding from a Russian university. Do you know if your work in Russia influenced its targeting of Facebook users for its misinformation campaign?

Answer. *No Response Provided.*

Question 2. It is unclear how many children and teens were affected by the Cambridge Analytica data breach. How many teens and children's data did you collect with your "this is my digital life" app?

Answer. *No Response Provided.*

Question 3. How did you use data about teens to profile and target them?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MAGGIE HASSAN TO ALEKSANDR KOGAN

Question. Mark Zuckerberg has said that he sees Facebook more as a government than a traditional company. Among other things, governments need to be transparent and open about the decisions they make. Many large institutions have set up independent systems—such as offices of inspectors general or ombudsmen and ethics boards—to ensure transparency and internally check bad decisions. Facebook has none of those controls. What kinds of independent systems should companies like Facebook have to publicly examine and explain their decision-making?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO ALEKSANDR KOGAN

Question 1. Cambridge Analytica Specifics: Cambridge Analytica whistleblower Christopher Wylie has stated quote "It's incorrect to call CA a purely data science company, or an algorithm company. It is a full service propaganda machine."

- Is that a fair assessment of your understanding of the organization prior to your involvement with them?
- What is your assessment in retrospect now?
- According to Mr. Wylie: "(Mr.) Kogan offered much cheaper, faster and better quality than anything else Cambridge Analytica had at their disposal, because the apps and the access to the friends' data beyond the initial users who engage with the app." Do you think that is a fair representation of the situation in 2014?

Answer. *No Response Provided.*

Question 2. Facebook Private Messaging: In a *Guardian* article, dated April 2018 [1], it is reported that your app could tap into private messages.

- Is this true?
- If true, please provide details into what information could be collected and how this information was stored, transferred, and used.
- What would be the value of this information?

Answer. *No Response Provided.*

Question 3. Nix Contacts/Comments

In an undercover video, Cambridge Analytica's CEO Alexander Nix has been identified to have been gloating about being a big time firm, with influence in elections all over the world.

- Is this true?

---

[1] *https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages*

- Did Mr. Nix ever say similar type of things directly to, or in front, of you in the course of your mutual relationship?
- Did Nix ever mention, or have you communicated about or with, WikiLeaks leader Julian Assange?

Answer. *No Response Provided.*

Question 4. Status and Timing of the Data Deletion

- Can you confirm whether Cambridge Analytica did in fact delete all necessary data after Facebook's request that Cambridge Analytica do so?
- Do you believe, as Facebook claims, that they had just discovered the violation of the contract when they requested the data be deleted?
- Did you provide the full or partial data you obtained through your agreement with Facebook to anyone else, other than Cambridge Analytica? If so, please detail who.
- Do you still have any data about Facebook users?

Answer. *No Response Provided.*

Question 5. Facebook Policy Changes: In April 2014, Facebook changed its policies so that users were no longer permitted to share friends' data with third party apps, they introduced more granular controls for data sharing, allowing users to pick and choose which data to disclose. Facebook also required all apps on its platform to go through a proactive review of their privacy policies and data needs before allowing them to collect user data. Preexisting apps on the platform were given until May 2015 to comply with the new policies. During this time gap or "grace period"—that is, from April 2014 to May 2015—"thisismydigitallife" may have been able to scrape friends' data without being in violation of Facebook policies. However, under the new policies that were effective for all apps in May 2015, Facebook claims that "thisismydigitallife" would not have been authorized to obtain the same amount of data it was able to collect under the previous policies.

Any time during this period, did you do any more aggressive data collection efforts before your broader access was constrained?

Answer. *No Response Provided.*

Question 6. Security of Kogan's Data: In a hearing in the Judiciary committee earlier this year Mr. Wylie stated that it would have been incredibly easy for hackers to access the data on your computer with a key logger. Intelligence services of nations hostile to the United States would no doubt desire to have access to that data.

How confident are you that, during your travels in Russia and elsewhere, that the data that you were carrying was not compromised?

Answer. *No Response Provided.*

Question 7. Nondisclosure Agreement: Facebook has claimed that the nondisclosure agreement that you signed was signed in June of 2016. This is several months after they claim they were made aware of the breach in December 2015.

Do you have any insight as to why this occurred in June 2016?

Answer. *No Response Provided.*

Question 8. Interactions with Facebook: During the hearing you stated that in the spring of 2015, months before the Guardian report, you raised concerns with Facebook that GSR's terms of service conflicted with Facebook's policy on data transfer. You stated that "we went through various ways of letting Facebook know" about this.

- Please provide as much information as possible as to the precise dates of these and other relevant interactions.
- Can you please describe, to the best of your recollection, the nature of these conversations and interactions, including any responses from Facebook.
- Please detail the dates of and nature of any interactions with Facebook as part of the company's app review process for any apps that you developed.
- Please provide information related to how Joseph Chancellor was involved in any of these interactions.

Answer. *No Response Provided.*

Question 9. Facebook Certifications: Facebook has claimed that it obtained written certifications from you, GSR, and other third parties (including Cambridge Analytica and SCL) declaring that all data they had obtained, and any derivatives, were accounted for and destroyed.

- Who signed these documents?
- Were they legally binding?
- Who drafted the documents?

Answer. *No Response Provided.*

Question 10. Other Partners: In his testimony before the Senate Judiciary Committee last month, Christopher Wylie suggested that you were also working with Russian-funded projects using Facebook data for trolling and psychological profiling.

- Do you have a response?
- Did you have any criteria for what entities you were willing to share data with?
- What were those criteria?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO ASHKAN SOLTANI

Question. Facebook Data Sharing Agreements

In the *New York Times* article about Facebook's agreements with device makers, you are quoted as saying: "It's like having door locks installed, only to find out that the locksmith also gave keys to all of his friends so they can come in and rifle through your stuff without having to ask you for permission."

Facebook argues that these agreements were perfectly legitimate and were necessary during the early days of the smartphone. What is your response?

Answer. Facebook promised users that they could limit the information they shared with third-party companies using the Facebook platform privacy settings. Yet, even after making that promise, Facebook permitted third-party companies—such as Blackberry—to circumvent users' privacy settings and access users' private information. In responses to public reporting, Facebook defended its decision by splitting hairs about which type of third party it originally meant, claiming that device manufacturers are different from app developers, and therefore were not of concern.

Facebook claims the partnerships were necessary, but in fact they were simply a business decision by the company to expand its platform to grow its user base. At its base, the decision was about business, not survival. Further, Facebook's claim of legitimacy is belied by the fact that it provided unequal access to its users to different companies. Some got more or less access to consumers' private information depending on the value of the partnership to Facebook. This business practice put growth before user privacy.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO ASHKAN SOLTANI

Question 1. FTC Consent Decrees and Facebook: In November 2011, Facebook agreed to a consent decree after the FTC found that the company had deceived consumers by sharing personal data with advertisers and making public information previously designated as private. Under the terms of its consent decree, Facebook was required to establish a comprehensive privacy program designed to address privacy risks and obtain audits to ensure that the privacy of consumers' information is protected. Between its failure to safeguard against misuse and its ineffective privacy controls, I believe that Facebook may have violated the terms of its consent decree, which I expressed to the FTC in an April letter. I look forward to Mr. Soltani's written response on other data collection or sharing practices that he believes warrant investigation by the FTC. I am additionally interested in Mr. Soltani's recommendations on how Congress can support the FTC on data privacy.

From your experience, does FTC staff review the reports mandated under the consent decree, such as to independently evaluate them for accuracy or completeness? What should the FTC be doing to ensure that consent decrees are effectively enforced?

Answer. The Federal Trade Commission has an independent division—the Division of Enforcement—responsible for enforcing Commission orders. This division is separate from those that bring initial actions—in this case, the Bureau of Consumer Protection. The Division of Enforcement oversees the business practices of covered entities and reviews outside reports to determine whether violations are taking place. In addition, they are tasked with enforcing *every* Commission order as well as the many idiosyncratic laws under the Commission's jurisdiction.[2] There are no

[2] For instance, the Enforcement Division must ensure that covered entities comply with labeling and country-of-origin requirements under the Textile and Wool Acts (15 U.S.C. § 70, et seq.; 15 U.S.C. § 68, et seq.), which creates obligations for labeling cloth. Fed. Trade Comm'n, *Threading Your Way Through the Labeling Requirements Under the Textile and Wool Acts, https://*

more than a dozen or so staff in this division at any given time. By necessity, they are largely generalists, not versed in the complex and rapidly developing challenges of technology.

Even if the staff were able to fully examine compliance with every Commission order, the assessments and reports provided by companies under consent order often fall well short of providing a clear and complete picture of privacy and data protection practices. As former FTC enforcement attorney Megan Gray wrote in a white paper earlier this year,[3] privacy assessments provided to the Commission are generally self-designed assertions from the company that it has a privacy policy and employees someone responsible for oversight. The orders generally do not require companies to demonstrate practical compliance with these policies. This leaves the Commission without any ability to determine whether a company actually follows its policies.

A proper oversight regime would mandate regular audits and reviews of companies under order by dedicated staff, including a mix of technologists and lawyers who could scrutinize a firm's rapidly changing practices to assess whether its practices and policies are in compliance with the consent decree.

Question 2. You helped to create the FTC's Office of Technology Research and Investigation. In your opinion, what further resources or authorities should Congress provide the FTC to protect consumers in the digital age?

Answer. The Federal Trade Commission should have a separate Bureau of Technology—similar to the Bureau of Economics—that would be responsible for consumer protection and competition concerns raised by emerging technologies. The elevation of the Office of Technology Research and Innovation to a full Bureau would reflect the changing business and consumer landscape in America, and would provide a meaningful boost to the Commission's capabilities in this space.

The Bureau should be led by a Chief Technologist with academic credentials, and should be fully staffed with technologists and technical analysts responsible for driving the Commission's research and enforcement agenda. Creating a center for technical expertise in the Commission would allow it to lead coordination and collaboration with other agencies engaged in technology policy—such as NIST, the FCC, SEC, CFPB, and NTIA—and would allow the Commission to explore highly technical challenges in consumer protection and competition, such as algorithmic discrimination, the development of artificial intelligence, and facial recognition deployment.

Question 3. Privacy Legislation: Across hearings and questions for the record, members of Congress have raised concerns about the data collection tactics used by Facebook that are not made clear to its users. As I stated during the hearing, I am interested in putting into place rules of the road for online privacy, taking into consideration the European General Data Protection Regulation. During the hearing Mr. Battelle and others offered support for the intent of GDPR, but expressed reservations about the implementation and unintended consequences. I look forward to any further thoughts from the panelists regarding how to implement data privacy rules in the United States.

In addition to any recommendations or comments on what types of legislation or other measures could help protect consumer privacy, what lessons and principles of the California Consumer Privacy Act and the GDPR should Congress consider in privacy legislation?

Answer. The California Consumer Privacy Act will not take force until 2020, so lessons from its implementation are limited. It is clear, however, that CCPA will provide consumers with meaningful choice about how their data are used and controls on how that data are shared. This is especially true for data given to third parties: the CCPA requires that businesses disclose to consumers information about who has the consumers' data and the ability for consumers to opt out of the further reselling of that data. CCPA provides a strong baseline for any potential Federal legislation, and should be considered a minimum set of requirements going forward.

The successful implementation of the GDPR shows us that companies are ready and able to comply with stronger protections for consumers. As Congress considers enacting Federal privacy legislation, it should remember that companies large and small are able to innovate and thrive at the same time they protect their users.

Technology is a fast-paced industry. Allowing states to continue to develop new ways to protect consumers—even as Congress considers its own legislation—will

---

www.ftc.gov/tips-advice/business-center/guidance/threading-your-way-through-labeling-requirements-under-textile#intro.

[3] Megan Gray, *Understanding and Improving FTC http://cyberlaw.stanford.edu/files/blogs/white percent20paper percent204.18.18.pdf*

provide companies, consumers, and Congress with the best outcome. Congress should avoid preemption.

New legislation should incentivize investment in privacy-protective technologies and practices, and should encourage or require companies to implement data minimization practices and reasonable data-use policies. Congress should also take steps to address the competitive aspects of privacy and data protection.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO ASHKAN SOLTANI

Question 1. What actions do you support by Congress, the Federal Election Commission, or the Federal Trade Commission to tighten and enforce rules to stop the election meddling we saw in 2016?

Answer. It's critical that Congress propose solutions to increase oversight of how technology is used to persuade or influence individuals. That oversight must take place whether influence is used for commercial purposes or, more importantly, to influence the democratic process. Instituting transparency and reporting requirements is an important first step in that oversight.

Companies should provide transparency into how platforms and social media display content to users, including decision-making processes for promoting advertisements and sponsored content. Transparency should extend beyond mere principles and instead should provide accountable metrics around ranking, promotion, and filtering. For example, platforms should implement oversight and redress procedures for flagging content, especially when determining that content is problematic or inauthentic. The FEC and FTC should take similar steps to ensure, respectively, that political advertising is not abused on platforms and that consumers are provided accurate and reasonably complete information about platform operations.

Question 2. Do you think the current Facebook political advertising transparency changes will prevent the widespread abuse of their digital advertising platforms by Russian government funded actors that we saw in the 2016 elections?

Answer. Facebook's transparency policy clearly does not go far enough to address a polarized political environment. As threats and the cultural ecosystem changes, minor tweaks simply do not do enough to challenge the systemic problems created by the abuse of platforms by foreign governments and other unscrupulous speakers. Indeed, just this week, reporters posing as U.S. Senators were able to purchase fake political advertising on behalf of all 100 members without any pushback from Facebook. Major social media sites have allowed an immense amount of coercive and abusive speech on their platforms, and should examine how to curtail that abuse—and protect users—without stifling the rights of legitimate speakers.

Question 3. Last year, Facebook released the Messenger Kids' application to serve as a safer space for children to chat online with each other. However, thus far, Facebook has not disclosed which 3rd parties have access to that data. How can Congress support the FTC to ensure that our children's data are not being shared with the unauthorized parties?

Answer. The FTC plays an important role in ensuring that children are protected online. In addition to their multitude of other missions, the Commission is responsible for enforcing COPPA—the Children's Online Privacy Act. As more and more children are exposed to online services, it is ever more important that the FTC has power and resources to investigate the proliferation of apps and services placed in front of—and directly targeted to—children. As the online marketplace for children's information grows, the FTC must be given commiserate resources, staff, and authority to ensure that children remain protected online.

Question 4. Facebook's standard operating procedure seems to be deny that a problem occurred, then admit a problem occurred and minimize the impact to consumers, and then disclose the impact is far greater than previously assumed. This is especially concerning in light of the recent news about its partnership with Huawei. While Huawei has assured us that it didn't collect any data about users, is there any way to verify this claim?

Answer. Without conducting an audit of either Facebook's or Huawei's servers, it is not possible to determine conclusively what data Huawei may have collected from Facebook. I am happy to discuss this issue further with your staff.

Question 5. How can Congress support the FTC in its effort to hold Facebook accountable for these breaches of consumer trust and national security?

Answer. Congress should provide the FTC with additional monetary and staff resources and the ability to conduct direct rulemaking to protect consumer privacy and cybersecurity.

Congress should also consider creating a formal Bureau of Technology at the FTC tasked with research and investigation of the underlying technology that impacts and complicates many of the democratic, consumer protection, and competition questions facing the FTC.

Question 6. In your testimony, you spoke about using a Blackberry to gain access to information that was deemed private. Is it conceivable that foreign actors, including Russians, have used this tool to gather large amount of data on American consumers? If so, what are the implications of this access?

Answer. It is certainly conceivable. Facebook is able to grant access to user information to any party it chooses. It may also provide third parties with the ability to circumvent users' privacy controls and access information that users seek to keep fully or partially private. This access is traditionally given via an Application Program Interface (API). If a rogue actor, such as a nation state or criminal enterprise, obtained API tokens granted to Blackberry, that rogue actor would have access to all the information Facebook permits that company to access, including information Facebook users attempted to keep private. The troves of information available to the rogue actor would allow them to create precise profiles on nearly any Facebook user and exploit those profiles at will.

Question 7. When Mr. Zuckerberg testified in from the Senate Commerce Committee, he declined to acknowledge Facebook's market power. Do you believe Facebook has any competition in the marketplace now?

Answer. In my opinion, there is no direct competitor to Facebook's combined suite of services and direct access to consumers. This is due in part to Facebook's rapid growth and dominance, and partly to the company's practice of acquiring nascent competitors before those growing companies can pose a threat to Facebook's business practices or user networks. The current market simply does not have a competitor for Facebook, and Facebook has taken active steps to ensure that remains so.

More broadly, there is no single economic actor that matches the breadth, depth, and scope of Facebook. Not only is Facebook the dominant social platform, but it is also one of the world's most popular mobile apps, and is the de-facto "single sign-on" provider online for millions allowing consumers use to log-in to other websites and services using their Facebook accounts instead of traditional usernames and passwords. Truly, it is difficult, if not impossible, to navigate online without encountering or interacting with Facebook.

Question 8. I am concerned about Onavo, a Facebook-owned "Virtual Private Network" app, and consumers' expectation of privacy when utilizing this app. Do you know if Facebook has access to information that would otherwise be private?

Answer. Facebook was certainly able to leverage its control of Onavo to learn about users' behavior and habits. This is exemplified by reporting that explains how Facebook was able to analyze mobile user traffic of Onavo users to determine that Snapchat and WhatsApp were growing in popularity with Onavo users. Facebook later built its own version of a popular Snapchat feature and acquired WhatsApp outright. This matches a well-documented pattern of Facebook using its own online tools to cut-off or acquire potential competitors.

This is not speculation: Facebook was forced to remove Onavo from the Apple App Store specifically because Facebook was using user data from the app to conduct analytics and marketing research, in violation of Apple's terms of service. The browsing and app-usage habits of Onavo users should have remained private, and would have if Facebook had not gone out of its way to examine them.

Question 9. Mr. Soltani, in your testimony, you stated that the only way users can object to particular privacy practices is to boycott a certain service. However, isn't it true that Facebook, and other entities, still gather data of consumers that are not on their platforms?

Answer. Facebook has confirmed that it does collect information on consumers who are not logged into the service as well as those who do not have Facebook accounts. For example, Facebook is able to uniquely track websites using their social widgets, including those that aren't part of the network. Any time a consumer sees a Facebook "Like" button on a page, that consumer is being tracked, voluntarily or no, by Facebook.[4]

---

[4] Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook,* Consumer Reports (Apr. 11, 2018), *https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook.*

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MAGGIE HASSAN TO ASHKAN SOLTANI

Question. Mark Zuckerberg has said that he sees Facebook more as a government than a traditional company. Among other things, governments need to be transparent and open about the decisions they make. Many large institutions have set up independent systems—such as offices of inspectors general or ombudsmen and ethics boards—to ensure transparency and internally check bad decisions. Facebook has none of those controls. What kinds of independent systems should companies like Facebook have to publicly examine and explain their decision-making?

Answer. Transparency and accountability are critical to any entity making decisions about what people see and experience on such a massive scale. As such, Facebook and other large companies should publish and commit to principles for how they will conduct governance—both of content and of users—on their platforms. Large platforms should take steps to ensure these should principles are not simply be policies on paper, but that they are meaningfully enacted and enforced. Principles should be subject to public comment and review, and should be based at least partially on consensus.

Facebook should appoint principals, such as ethics officers and additional compliance staff to ensure governance is conducted appropriately and transparently. At the very least, Facebook should demonstrate its commitment to acting ethically by appointing a Chief Ethics Officer to oversee internal review of programs from an ethical perspective. A high-ranking corporate officer—with adequate staff and resources—would show a commitment to ethical and transparent decision making and would improve the quality of Facebook products and services.

Facebook should also appoint ombudsmen to interface with local communities and stakeholders to ensure moderation and governance decisions reflect the needs and expectations of all those who use the service. Governance needs vary at different levels and in different contexts, and a major platform—like a government—must respond to all the many needs of its users. Ensuring that users have a voice in decision-making will provide Facebook with better, safer, and more responsive policies.

No principles or outreach can be truly effective unless Facebook and other platforms ensure transparency and accountability for their decisions. In addition to publishing principles and soliciting community input, Facebook and others must provide formal mechanisms for redress. Platforms should be transparent about why and when they remove accounts, and should submit reports on takedowns. They should ensure that users have meaningful recourse to appeals when content is removed. And platforms should cooperate with governments to ensure safe online spaces while respecting local rights and values.

Facebook and other platforms are enormous, complex shared spaces. Platform procedures and decisions must reflect the many expectations and values of the users they serve in the United States and worldwide. Users must be given tools to understand how platforms will treat their accounts and their content, and must be allowed to challenge those decisions when there is error or abuse.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO ASHKAN SOLTANI

Question 1. Facebook Audits: On April 4, 2018, following the public controversy over Cambridge Analytica's use of user data, Facebook announced several additional changes to its privacy policies. The changes include increased restrictions on apps' ability to gather personal data from users and also a policy of restricting an app's access to user data if that user has not used the app in the past three months. In addition, Facebook has committed to conducting a comprehensive review of all apps gathering data on Facebook, focusing particularly on apps that were permitted to collect data under previous privacy policies. Facebook will also notify any users affected by the Cambridge Analytica data leak.

What steps can the government take to ensure that there is proper oversight of these reviews and audits?

Answer. First and foremost, companies under consent decree with the Federal Trade Commission should be required to provide all relevant information on their privacy practices—not just policies. Information from Facebook about its review—including how it conducts that review, what information is impacted, and how it intends to address the results—should be supplied to the Commission so that the FTC can make appropriate decisions about enforcement moving forward. The government should also require that reviews and audits include meaningful third-party review and examination to ensure that ongoing issues are spotted and addressed.

Question 2. From a technical standpoint, how effective are forensic methods at ascertaining information related to what data was transferred in these cases?

Answer. After Facebook was outed by the press, it was able to understand the extent of Cambridge Analytica's misuse of the Facebook API by examining logs of access to that service. This type of review can expose other types of misuse as well, so long as log reviews are conducted. Previously, Facebook was not conducting thorough reviews of these logs: the lack of review allowed abusive practices to continue for years without notice. This is especially concerning because log review is basic cyber hygiene, and should be part of any comprehensive security program.

Log examination and review are highly effective tools for discovering abuse—if they are used. Log records show how an API is used, and how it is misused. However, private companies may choose to not conduct these reviews for myriad reasons—the company may decide they are too expensive, or they simply may not value the insights they provide.

But examining API use is far from the full picture. While companies should monitor API usage, they should also take steps to monitor all potential points of entry, no matter how unlikely. Simply securing the front door is inadequate if the back windows are unlocked and unmonitored.

Question 3. Facebook Private Messaging: Can you explain if and, if so, how Facebook monitored private chats and what it did with that information?

Answer. Facebook monitors private chats for a number of reasons, including did monitor private chats. For example, Facebook monitors chats looking for sexual predators and child pornography in order to remove them from the platform.[5] However, in my research, I've also identified that Facebook monitored users chats to determine their interests, and used its tools to determine when users mentioned a particular website or "page." Facebook did this in order to gauge users' interests in particular topics and provide that information to third parties.[6]

Question 4. Do you believe users were generally aware of this?

My belief is that users were generally not aware that Facebook was monitoring their private conversations in order to tell marketers what websites and products they were interested in. Typically, "private chat" connotes just that. Intercepting all communications likely falls out of consumer expectations for such a service.

Question 5. Technology for Consumer Protection: Are there any technological solutions being developed that can help address some of the issues of consumers' privacy being violated online?

Answer. A variety of tools are available or being developed that allow companies to operate without needing to violate consumers' privacy online. Technologists have made a great number of innovations in this space, such as zero-knowledge proofs[7] and homomorphic encryption.[8] There are also proven methods to deliver advertising to consumers without violating their privacy, such as DuckDuckGo which does not track users' search histories, or Adnostic,[9] which can show ads without revealing users' private behaviors. Any legislation should incentivize innovation in this space and encourage exploration of new privacy-preserving business models.

Question 6. Net Neutrality: Mr. Soltani, as you know recently the FCC voted to repeal net neutrality rules that prevent Internet service providers from blocking or throttling content, and it will now be up to the FTC to enforce broad anti-competition rules against ISPs.

As the former CTO at the FTC, can you describe the level of specific Internet expertise at the Commission and resources typically available to be a sufficient enforcement entity to cover any potential future anti-competitive behavior by Internet service providers?

Answer. While the Federal Trade Commission has insights regarding peering arrangements and experience with privacy concerns related to Internet Service Providers, it could certainly gain even more credibility by hiring dedicated technologists

---

[5] Kashmir Hill, *Yes, Facebook Scans Users' Private Conversations Looking For Sexual Predators and Child Porn,* Forbes (July 13, 2012), *https://www.forbes.com/sites/kashmirhill/2012/07/13/yes-facebook-scans-peoples-private-conversations-looking-for-sexual-predators-and-child-porn.*

[6] James R. Hood, *Facebook Agrees to Stop Reading Your Messages,* Consumer Affairs (Mar. 3, 2017), *https://www.consumeraffairs.com/news/facebook-agrees-to-stop-reading-your-messages-030317.html.*

[7] Matthew Green, *Zero Knowledge Proofs: An Illustrated Primer* (Nov. 27, 2014), *https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer.*

[8] Neal Ungerleider, *What's Homomorphic Encryption And Why Did It Win A MacArthur Genius Grant?,* Fast Company (Sept. 17, 2014), *https://www.fastcompany.com/3035879/whats-homomorphic-encryption-and-why-did-it-just-win-a-macarthur-genius-grant.*

[9] *https://crypto.stanford.edu/adnostic/*

tasked with better understand how ISPs operate. The Federal Trade Commission would greatly benefit from a separate Bureau of Technology—similar to the Bureau of Economics—that would be responsible for consumer protection and competition concerns raised by emerging technologies. The elevation of the Office of Technology Research and Innovation to a full Bureau would reflect the changing business and consumer landscape in America, and would provide a meaningful boost to the Commission's capabilities in this space.

Question 7. In your opinion, are these resources sufficient?

Answer. Commission staff simply cannot police the entire Internet ecosystem. New technologies and products are introduced to the market at a rapid pace, and staff, with limited resources and many obligations, do not have the time or expertise to remain current. The Commission would need significant additional resources—people—to be an effective "cop on the beat" for ISPs along with its other obligations.

Question 8. If not, how can we better provide appropriate staffing and resources for this purpose?

Answer. The Commission should be provided with additional financial and human resources that match the rapid expansion and development of the Internet ecosystem.

Question 9. Data Retention: What should we, as legislators, should be thinking about to verify that—when Americans are told that their data has been destroyed—that deletion can actually be confirmed?

Answer. Because of the nature of digital data, it is difficult to prove definitively that the data has not been copied, removed, or reposted prior to deletion. Without creating a "right to audit" such as that in the European Union, it will be difficult, if not impossible, to know for certain that a company has deleted data as required. Without that right, consumers and regulators would need to take companies at their words.

Any policy solution must incentivize companies to respect deletion rights. This included mandating stiff penalties for violations, including violating consumer expectations of what deletion entails. If companies violate those provisions, they should be subject to audit and other intrusive monitoring practices to ensure future compliance.

Question 10. Law Enforcement: During the hearing we had a brief discussion on the balance between privacy and sharing data with law enforcement.

What should companies keep in mind to ensure that they can appropriately assist in law enforcement investigations?

Answer. Companies must ensure they retain data for use by law enforcement while also respecting the rights of users to have data remain private. If companies do hold consumer data for long periods of time, that storage must meet heightened standards of security and privacy to ensure the data remains safe. Any company holding data for extended periods of time—whether to assist law enforcement or for other reasons—must provide clear and transparent reasons for why it is holding that information.

Question 11. As lawmakers, what should we be aware of as we try to strike the right balance between privacy and safety in this area?

Answer. It is essential to allow law enforcement to continue its mission while simultaneously improving consumer privacy. This is not a static field, however. Surveillance and other law enforcement technology is becoming increasingly less expensive and easier to deploy. I have written on this subject,[10] and the concept was recently addressed head-on by the Supreme Court in Carpenter v. United States.[11] As lawmakers consider the balance in this space, they must remain aware that the development of technology will always act to strip privacy rights from individuals and allow the government access to previously inaccessible actions and behaviors.

○

[10] Ashkan Soltani, *The Cost of Surveillance* (Jan. 9, 2014), *https://ashkansoltani.org/2014/01/09/the-cost-of-surveillance.*

[11] Carpenter v. United States, No. 16–402, 585 U.S. __(2018).