AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–656

DATA SECURITY AND BUG BOUNTY PROGRAMS: LESSONS LEARNED FROM THE UBER BREACH AND SECURITY RESEARCHERS

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

FEBRUARY 6, 2018

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

37–302 PDF WASHINGTON : 2019

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

DATA SECURITY AND BUG BOUNTY PROGRAMS: LESSONS LEARNED FROM THE UBER BREACH AND SECURITY RESEARCHERS

TUESDAY, FEBRUARY 6, 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 p.m. in room SR–253, Russell Senate Office Building, Hon. Jerry Moran, Chairman of the Subcommittee, presiding.

Present: Senators Moran [presiding], Blumenthal, Blunt, Nelson, and Cortez-Masto.

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

Senator MORAN. Good afternoon. Welcome to the Consumer Protection Product Safety, Insurance, and Data Security Subcommittee's Hearing on "Data Security and Bug Bounty Programs."

The Subcommittee will come to order. Thank you all for being here today to discuss the October 2016 Uber data breach and the allegations against the company regarding impermissible payments to concealed security incident through its Bug Bounty Program.

A bug bounty is a reward offered to someone outside of the company who identifies an error or vulnerability in a computer program or system in connection with the Coordinated Vulnerability Disclosure Program.

The Committee plans to examine the value of these innovative programs and other coordinated approaches to identify cyber vulnerabilities and prevent the types of instances that have occurred and, unfortunately, will probably occur in the future.

In late 2016, Uber was notified by anonymous sources that certain archived copies of its database had been compromised. According to a letter in response to an inquiry made by this Committee, in partnership with the Senate Finance Committee, Uber's Security Team "took immediate steps to respond to and limit the impact of the incident," including identifying the parties responsible and paying a $100,000 to them in exchange for assurances that the compromised data would be deleted.

I have a letter and Uber's response that I would ask unanimous consent to be submitted for the record. Without objection.

[The information referred to follows:]

United States Senate
WASHINGTON, DC 20510

November 27, 2017

Mr. Dara Khosrowshahi
Chief Executive Officer
Uber Technologies, Inc.
1455 Market Street
San Francisco, CA 94103

Dear Mr. Khosrowshahi:

We write today regarding reports that, in late 2016, Uber learned that it had suffered a significant data security incident. Hackers apparently accessed user data including the names and driver's license numbers of about 600,000 drivers in the United States as well as the personal information of 57 million Uber users around the world, including names, e-mail addresses, and mobile phone numbers.[1]

Perhaps more troubling, several media reports indicate that, rather than report the incident to regulators or to affected customers, Uber instead paid $100,000 to the hackers to delete the stolen data, allegedly to conceal the breach.[2]

The company maintains that its outside forensic experts have not seen any indication that customer trip location history, credit card numbers, bank account numbers, Social Security numbers, or dates of birth were downloaded.[3] Nevertheless, the nature of the information currently acknowledged to have been compromised, together with the allegation that the company concealed the breach without notifying affected drivers and consumers, and prior privacy concerns at Uber, makes this a serious incident that merits further scrutiny.

In January 2015, Uber released a report entitled "Review and Assessment of Uber's Privacy Program."[4] The review that Uber's outside counsel conducted determined that Uber had in place "appropriate policies and procedures" in several areas, including data security, incident management and response, data retention, and accountability.[5] Though a technical audit was not part of this review, the report found that, "Uber has put in place and continues to develop a data security program that is reasonably designed to protect Consumer Data from unauthorized

---

[1] Dara Khosrowshahi, *2016 Data Security Incident*, UBER NEWSROOM (Nov. 21, 2017), http://www.uber.com/newsroom/2016-data-incident.
[2] *See, e.g.*, Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, BLOOMBERG TECH., Nov. 21, 2017, http://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.
[3] Khosrowshahi, *supra* note 1.
[4] Hogan Lovells, Review and Assessment of Uber's Privacy Program (Jan. 2015), https://newsroom.uber.com/wp-content/uploads/2015/01/Full-Report-Review-and-Assessment-of-Ubers-Privacy-Program-01.30.15.pdf.
[5] *Id.* at 1.

access, use, disclosure, or loss."[6] It further details administrative, technical, and physical safeguards for data protection, as well as company policies for reporting and responding to data breaches.[7] Despite the safeguards in place, according to recent reports, Uber's board commissioned an investigation by an outside law firm, which discovered the recently revealed hack and the failure to disclose it.[8]

Additionally, the Federal Trade Commission (FTC) announced on August 15, 2017, that Uber agreed to a consent order addressing its privacy and data security practices. Among other things, the order prohibits Uber from misrepresenting the extent to which it protects the privacy, confidentiality, security, or integrity of any personal information.[9] The order also requires Uber to implement a comprehensive program to protect the privacy and confidentiality of the personal information it collects and maintains.[10]

Our goal is to understand what steps Uber has taken to investigate what occurred, restore and maintain the integrity of its systems, and identify and mitigate potential consumer harm and identity theft-related fraud against Federal programs. Accordingly, we request answers to the following questions:

1. On what date did Uber first learn that hackers accessed user data stored on a third-party cloud-based service?
2. How many consumers does the incident affect, including riders and drivers? Please describe Uber's efforts to identify and provide notice to the affected individuals.
3. With respect to the incident, what types of data does Uber believe to have been compromised? To what extent does the data include sensitive personal information?
4. Did Uber authorize payments to outside parties in connection with the incident? If so, please provide additional details, including the amounts, dates, method of transfer, as well as the purpose of such payments, including whether the purpose of such payments was, even in part, to conceal the incident itself. Who authorized these payments?
5. Which regulators has Uber notified about the incident? On what dates did these notifications occur?
6. Beyond monitoring affected accounts, what steps has Uber taken to identify and mitigate potential consumer harm associated with this incident?
7. What steps has Uber taken to ensure compliance with its obligations under the FTC order, such as its obligation to establish, implement, and maintain a comprehensive privacy program?

---

[6] *Id.* at 2.
[7] *Id.* at 22-25.
[8] Newcomer, *supra* note 2.
[9] Press Release, Fed. Trade Comm'n, Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.
[10] *Id.*

8. Did Uber disclose the incident to the FTC during the agency's investigation that led to the consent order? If so, when? If not, why not?
9. What personnel actions has Uber taken in response to the incident? Please provide specific details.
10. Please provide a detailed timeline of events, including Uber's initial discovery of the incident, forensic investigation and subsequent security efforts, notifications to law enforcement agencies and regulators, as well as any notification to affected consumers.
11. Uber has maintained that the hackers did not download social security numbers. Did the breach involve the compromise of social security numbers in any way? Please provide a complete description, including any related forensic analysis.

We look forward to receiving your responses as soon as possible, but by no later than 5:00 p.m. on December 11, 2017. In addition, please direct your staff to make arrangements to brief our staffs on this matter by no later than December 1, 2017. Thank you for your prompt attention to this matter.

Sincerely,

JOHN THUNE
Chairman
Committee on Commerce, Science, and Transportation

ORRIN HATCH
Chairman
Committee on Finance

JERRY MORAN
Chairman
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

BILL CASSIDY, M.D.
Chairman
Subcommittee on Social Security, Pensions, and Family Policy

cc: The Honorable Bill Nelson, Ranking Member
Committee on Commerce, Science, and Transportation

The Honorable Ron Wyden, Ranking Member
Committee on Finance

The Honorable Richard Blumenthal, Ranking Member
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

The Honorable Sherrod Brown, Ranking Member
Subcommittee on Social Security, Pensions, and Family Policy

UBER
December 11, 2017

Hon. JOHN THUNE,
Chairman,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Hon. ORRIN HATCH,
Chairman,
Committee on Finance,
Washington, DC.

Hon. JERRY MORAN,
Chairman,
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Protection,
Washington, DC.

Hon. BILL CASSIDY, M.D.,
Chairman,
Subcommittee on Social Security, Pensions, and Family Policy,
Washington, DC.

Dear Chairmen Thune, Hatch, Moran, and Cassidy:

Thank you for your letter dated November 27, 2017, requesting more information regarding the data security incident we announced on November 21, 2017. Thank you also for the interest shown and the time taken by your committee staff during our briefing on December 4, 2017. As Uber's new CEO, I am committed to setting our course for the future, which begins with building a company that everyone can trust and be proud of. For that to happen, we have to be honest and transparent as we work to repair our past mistakes.

I appreciate the depth and range of interest reflected in the questions posed in your letter and at our briefings. As we described when we met with your staff, we think it is important for you to get the facts from us directly. Our work on this matter remains ongoing, but we are now able to share the information below, and we appreciate the opportunity to share more as it develops.

On November 14, 2016, Uber's security team received e-mails from an anonymous individual who claimed to have accessed Uber data and demanded payment. Uber investigated and determined that the individual and another person working with him had obtained access to certain archived copies of Uber databases and files located on Uber's private cloud data storage environment on Amazon Web Services. Uber determined the means of access, shut down a compromised credential, and engaged in communications with the outside actors. To the best of Uber's knowledge, the outside actors' access began on October 13, 2016, and there was no further access by the actors to Uber's cloud storage after November 15, 2016.

Uber's security team took immediate steps to respond to and limit the impact of the incident, including engaging in immediate and then ongoing communications with the original outside actor and a second individual subsequently identified to have been working with him. Uber agreed to pay the money demanded in exchange for an agreement to delete the data. Uber eventually paid $100,000 to the two individuals combined. The payment was made in December 2016 through HackerOne (*www.hackerone.com*), which Uber uses for its Bug Bounty program. Uber also worked to identify the real names and identities of the outside actors. It was successful in this effort, and it thereafter engaged in further communications with the two individuals using their real identities, including having them sign assurances that the data was destroyed. Although Uber mitigated damage precipitated by the breach, two of the Uber employees who led the response failed to disclose the incident to the appropriate parties. Uber does not know why these individuals failed to discharge properly their responsibility, but they were terminated as a result.

Mandiant, an independent cybersecurity firm, conducted a forensic analysis of the data at issue. Mandiant found no indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded. They found that the data includes:

- Information pertaining to approximately 57 million users (both riders and drivers) worldwide, including approximately 7.7 million drivers. Approximately 32 million of these individuals are outside the United States. Approximately 25 million users are inside the United States.
- For nearly all users, the downloaded files included names, e-mail addresses, and mobile phone numbers.
- In some cases, the files also included other information collected from or created about users by Uber, such as Uber internal user IDs (UUIDs); the UUIDs of a user who invited another user to sign-up with Uber or whom users shared rides with if they had opted into certain programs; a small number of short driver-related notes; certain one-time locational information, such as the lati-

tude and longitude corresponding to the location where the user first signed up for the Uber service; and other account information, including user tokens and hashed and salted versions of user passwords.

- For approximately 600,000 of the 7.7 million drivers, the files also included a driver's license number. Virtually all of these individuals are in the United States.

Uber provided individual notice to drivers with driver's license numbers in the data set starting on November 22, 2017, in most cases by mail but via e-mail if Uber has no mailing address for the individual on file. That notification offered one-year complimentary credit and identity theft protection services from Experian and provided information on how to sign up. Uber also provided information pages for *riders* and *drivers* on its website. Uber notified the United States Attorney's Offices for the Southern District of New York and for the Northern District of California, the Federal Trade Commission, the attorneys general of states with a regulator notice requirement in their data breach law, and the Dutch Autoriteit Persoonsgegevens (data protection authority, our lead regulator for user data outside the United States) on November 21, 2017. Uber is continuing to provide information as requested on an ongoing basis to regulators, law enforcement, and government entities worldwide. We note that some of your questions relate to other ongoing legal proceedings and investigations to which the company is a party, including the Federal Trade Commission's ongoing investigation, which remains open. We do not here comment on other ongoing legal proceedings and investigations.

In addition to the steps taken to confirm the data taken had been destroyed, Uber has not seen evidence of fraud or misuse tied to the incident; it is monitoring the affected accounts and has flagged them for additional fraud protection. As to Uber's privacy and data security practices generally, Uber's privacy policies detail what information it collects relating to riders and drivers and how it uses and discloses that information. Uber's current privacy policy is available at *https://privacy.uber.com/policy*, and that page also contains a link to Uber's previous policy, dated from 2015. (Uber's 2013 privacy policy is available on *archive.org* as well.) Uber provided notice of both the 2015 and 2017 revisions by e-mail to users. Uber's data security practices include access controls, multi-factor authentication, credential management systems, and use of encryption in transit and, where technically feasible, at rest. This particular incident (as we discussed in our recent briefings with your staff) nonetheless occurred because, unfortunately, the outside actors determined valid Uber login credentials for a particular workspace. After this incident (and well before providing notice of it in November 2017), Uber put in place several additional protections designed to mitigate the chance that the same form of intrusion could succeed today, such as adding two-factor authentication to one of the services that was involved in this incident.

Thank you for the opportunity to share this information with you. Please know that we take this matter very seriously, and Uber is available to help answer any additional questions you may have.

Sincerely,

DARA KHOSROWSHAHI,
CEO,
Uber Technologies, Inc.

Senator MORAN. An independent forensics analysis found that the exposed data included information pertaining to approximately 57 million users in total, both drivers and riders, 25 million of those affected users were from the United States, and driver's license numbers of about 600,000 drivers were compromised in the breach.

The fact that the company took approximately a year to notify impacted users raises red flags within this committee as to what systematic issues prevented such time-sensitive information from being made available to those left vulnerable.

Additionally, my colleagues and I seek specific clarification as to what policy safeguards are currently in place to prevent bug bounty programs from being used as extortion pay-out mechanisms in the future.

These substantive concerns, however, should not completely outweigh the overall utility of this innovative crowd-sourced approach that many industry actors have taken to proactively identify chinks in their technological armor through effectively administered bug bounty programs and other cyber vulnerability disclosure efforts.

As the American public becomes more and more dependent and dependent on innovative technologies to complete everyday tasks, cyber security vulnerabilities pose a direct threat. Whether it's through a critical telehealth monitoring system, autonomous vehicle transporting your family, or access to personally identifiable information, cyber threats are continuously evolving with the technology we rely on.

My goal for this hearing is to find out exactly what prevented Uber from immediately notifying its users who are impacted by the 2016 breach, the specifics of the related payments and what steps Uber is taking internally to improve its notification protocols.

I also want to have a larger discussion of how vulnerability disclosure programs, like bug bounties, can be used effectively to deter cyber threats from harming consumers.

It's my pleasure to introduce our panel today and I again appreciate, as I expressed to you personally, my gratitude for your presence here today.

Mr. John "Four" Flynn is the Chief Information Security Officer for Uber Technologies. He's an expert in information security with over 10 years' experience in the field, including leading Infrastructure Security at Facebook and managing Security Operations at Google.

Mr. Marten Mickos is the Chief Executive Officer of HackerOne, which is a leading bug bounty firm in the country, serving a variety of government and private sector clients, including Uber, and administering their Crowd Source Vulnerability Disclosure Programs.

Ms. Kate Moussouris is the Founder and CEO of Luta Security, Inc., which advises its clients on vulnerability coordination programs and applicable internal company policies.

And, finally, Mr. Justin Brookman is the Director of Consumer and Technology Policy for the Consumers Union, which is an independent nonprofit consumer organization. In his role, he focuses on policies related to consumer data privacy security.

I look forward to the testimony of these experts on our witness panel.

I either now turn to the Ranking Member of the Full Committee or the Ranking Member of the Subcommittee for their opening remarks.

Gentlemen. The Senator from Connecticut.

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

Senator BLUMENTHAL. Thank you. Thank you very much, Mr. Chairman, and I'd like to thank you and the Chairman as well as our Ranking Member for holding this hearing, which is truly of paramount importance to consumers in our country.

There ought to be no question here that Uber's payment of this blackmail without notifying consumers who were gravely at risk

was morally wrong and legally reprehensible and violated not only the law but also the norm of what should be expected.

At the same time that Uber was negotiating with its blackmailers, it also was speaking with the Federal Trade Commission for a smaller 2014 breach affecting the personal information of more than a 100,000 Uber drivers.

Drivers and riders were not informed of the breach that brings us here today. Neither were law enforcement authorities. It was not only kept secret but the company paid those hackers a $100,000 ransom to destroy evidence and keep quiet. In effect, it was almost a form of obstruction of justice.

The Online Trust Alliance says that 93 percent of all breaches in 2017 did not stem from software vulnerabilities. They were the result of poor security protocols, like failing to update software, use e-mail authentication, and training people to recognize phishing attacks. These kinds of weaknesses are readily correctable and the industry has a responsibility for doing it.

We've had repeated hearings and we ought to be demanding more action of law enforcement authorities as well as the industry over the years. In fact, we've had one hearing after another focused on data breaches. Very recently, we heard from the current and former heads of Equifax and Yahoo following their historic breach disasters.

A piecemeal after-the-fact approach would be better served if the Commission, the Federal Trade Commission, were able to prescribe rules that prevent these kinds of data breaches by requiring reasonable security practices in the first place and that's why the Ranking Member and I, Ranking Member Nelson, who's here today, reintroduced the Data Security and Breach Notification Act.

This bill directs the FTC to develop robust, flexible rules that require businesses to adopt reasonable security protocols to protect consumers' personal information from unauthorized access and establish strong breach notification requirements.

Whether driving a ride-share or calling a ride-share, individuals expect companies collecting their sensitive personal information to do everything in their power to protect their data and their security and privacy, notify them promptly when there is a breach that endangers those consumers and riders.

These kinds of expectations are not unreasonable or inflated. These expectations are realistic. They are commonsense measures that all Americans have a right to expect, and I look forward to hearing from the witnesses.

Thank you, Mr. Chairman.

Senator MORAN. Thank you, Senator.

The Senator from Florida, we're honored to have the Ranking Member of the Full Committee with us today, Senator Nelson.

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

Senator NELSON. Mr. Chairman, thank you very much, and what Senator Blumenthal has just said, the legislation is out there.

We will continue to work with the Chairman of the Full Committee, Senator Thune, in order to try to get meaningful data secu-

rity legislation, but any such bill cannot simply cater to corporate interests.

A bipartisan bill must provide consumer protections that are better than is in the current law and why is this? Well, this hearing today is just the latest edition in a long history of hearings that this Full Committee has held on high-profile data breaches.

Uber now joins Equifax, Yahoo, Target, Sony, and the University of Maryland, among others, as a breached entity telling a story to this committee and to Congress, and this story at this hearing only once again underscores the need for the comprehensive and strong Federal legislation to provide the protections.

Currently, the FTC is the key Federal agency that's bringing enforcement actions against the breached companies that have collected and stored vast amounts of consumer data, unfortunately, with lax security standards.

A myriad of state laws currently provide American consumers with a limited degree of protection. So we should not adopt Federal legislation that undercuts the FTC's existing longstanding well-established authority nor should we consider a bill that eviscerates all state legal protections and replaces them with weak Federal standards.

From this Senator's standpoint and I think Senator Blumenthal's, we can support only a data security bill that provides consumers with protection that are stronger than the current ones. It would be better for Congress to pass no bill than to pass a bill that provides less protections to the consumers compared to the status quo.

So thank you, Mr. Chairman, for having this hearing.

[The prepared statement of Senator Nelson follows:]

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

Today's hearing is the latest edition in a long history of hearings that the Commerce Committee has held on high profile data breaches. Uber now joins Equifax, Yahoo, Target, Sony, and the University of Maryland, among others, as a breached entity telling its story to this committee and to Congress. And this story at this hearing only once again underscores the need for comprehensive and strong Federal legislation that will provide adequate protections to consumers.

In this regard, Senator Blumenthal and I have once again introduced such legislation, the Data Security and Breach Notification Act, which would require companies to secure their data and to promptly notify consumers when there is a breach.

The bill would also impose criminal penalties on corporate officials that willfully disguise breaches from the public, and it would provide for robust enforcement by the Federal Trade Commission and state attorneys general working together to hold companies accountable.

As in previous Congresses, I will continue to work with Chairman Thune and other interested members of the committee to craft bipartisan and meaningful data security legislation.

However, any such bill cannot simply cater to corporate interests. A bipartisan bill *must* provide consumer protections that are *better* than what is in current law.

Currently, the FTC is the key Federal agency that is bringing enforcement actions against breached companies that collected and stored vast amounts of consumer data with lax security standards in place. And a myriad of state laws currently provide American consumers with a limited degree of protection from data breaches.

We should *not* adopt Federal legislation that undercuts the FTC's existing, longstanding and well-established authority; nor should we consider a bill that eviscerates all state legal protections and replaces them with weak Federal standards.

From my standpoint, I can only support a data security bill that provides consumers with protections that are stronger than current ones. It would be better for

Congress to pass no bill at all than pass a bill that provides consumers with less protections under the status quo.

Thank you again, Mr. Chairman. I look forward to hearing from our witnesses.

Senator MORAN. You're welcome, Senator Nelson. Thank you for joining us.

We're now ready for the testimony of our witnesses, and I would call on Mr. Flynn for his opening statement.

Thank you.

STATEMENT OF JOHN FLYNN, CHIEF INFORMATION SECURITY OFFICER, UBER TECHNOLOGIES, INC.

Mr. FLYNN. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member Blumenthal, and members of the Subcommittee, my name is John Flynn, and I serve as the Chief Information Security Officer of Uber.

I'm grateful for the opportunity to testify today regarding bug bounty programs, the 2016 data security incident at Uber, and lessons that we have all learned from this incident.

I'm honored to be here with an esteemed panel of people who have brought such an important security practice to companies worldwide.

Today, I'd like to focus on three topics. First, bug bounty programs and the important role they play in the never-ending battle against cyber threats. Second, the 2016 data security incident at Uber where I worked to determined how the intrusion occurred and close the gaps that the intruders exploited. Third, the lessons learned and additional layers of protections that we've implemented.

Bug bounty programs are a critically important tool. In addition to internal security efforts that are widely used as part—they are widely used as part of a comprehensive data security program. Bug bounty programs are an invitation to outside experts to search for vulnerabilities and report them. In exchange, companies offer rewards in recognition of that work.

Monetary bounties can range from hundreds of dollars to hundreds of thousands of dollars. Some companies offer non-monetary rewards, including branded apparel or public recognition.

Because of the security benefits of bug bounty programs, many major technology companies use them, including Uber, Google, Facebook, Microsoft, and others. The U.S. Government also has bug bounty programs, including at the Department of Defense.

Since we publicly launched our program in 2016, Uber's Bug Bounty Program has assisted in resolving more than 800 vulnerabilities and paid about $1.3 million in bounties. It has achieved very significant improvements for a relatively modest expenditure, including addressing a bug in the SSH Authentication System and a remote code execution bug in one of our websites.

The 2016 data security incident unfolded in a way that's entirely different than a typical bug bounty. On November 14, 2016, our Security Team received e-mails from an anonymous individual who claimed to have access to Uber data and demanded a six-figure payment.

We investigated the incident and assembled an Incident Response Team. The team of technical experts, which I directed,

quickly determined the means of access and shut down the compromised credentials. Specifically, our first step was to validate the intruder's claims. We determined that the data came from backup files stored in an AWS S3 bucket.

We next determined the intruder gained access to AWS S3 through credentials contained within code on a private repository on GitHub. Despite the limited information, we locked down the point of entry within 24 hours.

Separately, our Chief Security Officer Joe Sullivan led an effort to identify the intruders, a process we call attribution. Although I was not directly involved, I understand that the Attribution Team used various methods, including forensics, to gather further information on the intruders.

It ultimately ascertained the identities of both intruders, made contact, and received assurances that the data had been destroyed.

As you know, Uber paid the intruders a $100,000 through HackerOne and our Bug Bounty Program. Our primary goal in paying the intruders was to protect our customers' data. However, this was not done consistent with the way our Bug Bounty Program normally operates.

In my view, the key distinction regarding this incident is that the intruders not only found a weakness, they also exploited that vulnerability in a malicious fashion to access and download data and made extortion demands.

We recognize that the Bug Bounty Program is not an appropriate vehicle for dealing with intruders who seek to extort funds from the company. My written testimony contains additional details regarding the contents of the data.

While the incident remains under the investigation by the company and others, I echo statements by Uber's new leadership that it was wrong to not disclose the breach earlier. We are working to make transparency and honesty core values of our company, which I am gratified to see.

Thank you again for the opportunity to appear and testify today. I would be happy to answer your questions.

[The prepared statement of Mr. Flynn follows:]

PREPARED STATEMENT OF JOHN FLYNN, CHIEF INFORMATION SECURITY OFFICER, UBER TECHNOLOGIES, INC.

Mr. Chairman, Ranking Member Blumenthal, and members of the Subcommittee, my name is John Flynn. Since July 2015, I have served as the Chief Information Security Officer for Uber Technologies, Inc. I am grateful for the opportunity to testify today regarding bug bounty programs, the 2016 data security incident at Uber, and lessons that we—and the broader technology community—have learned from that incident. I am honored to be on such an esteemed panel with people who have brought such an important security practice to companies worldwide.

Before addressing today's topics, I would like to tell you a little about myself. My parents were USAID diplomats and Peace Corps volunteers. After studying computer engineering at the University of Minnesota, I too joined the Peace Corps. As a Peace Corps volunteer, I served for more than two years in Belize, where I helped lead a program that ensured teachers had access to computers and I taught classes on information security. After the Peace Corps, I attended night classes to obtain a master's degree in computer science while working full time as a Security Engineer at the George Washington University here in Washington.

Before joining Uber, I held positions as an Information Security Manager at Google, and as an Information Security Director at Facebook. I have spent over a decade working on highly technical data security issues, during a period in which

data security has expanded dramatically as a field and as a paramount priority for the technology industry and the country.

I would like to focus on three topics in my testimony today. *First,* I have significant experience with bug bounty programs from working for multiple companies, and will explain the important role that such programs play in the never-ending battle against cyber threats. *Second,* I will provide my perspective on the 2016 data security incident at Uber. My primary involvement in that matter was on the technical side, working under our chief security officer, and leading the effort to determine how the intrusion occurred and then to close the gaps that intruders exploited. While I am in a strong position to address the technical aspects of that incident, I was not actively involved in the process of identifying the intruders or interacting with the intruders once they were identified by others. *Third,* we learned valuable lessons from the 2016 incident, and I will describe the additional layers of protection and other enhancements that we have implemented to secure our users' data and minimize the risk of future intrusions.

Importance of Bug Bounty Programs

Bug bounty programs are a critically important tool and widely used as part of comprehensive data security programs. Of course, bug bounty programs do not take the place of dedicated internal security teams who work throughout the entire software development lifecycle to detect and repair vulnerabilities. At Uber, there are multiple teams of specialized experts constantly working to ensure that our systems are secure. My team consists of more than 100 people with experience in technical areas of security. Our security efforts generally involve the following: (1) controlling access to our systems and services; (2) using security by design principles during the planning process; (3) auditing and testing code during development and throughout its lifecycle; (4) monitoring for threats; and (5) managing ongoing reinforcement and patching processes to protect our systems and software from reported vulnerabilities.

Bug bounty programs are a useful addition to these steps. Let me briefly explain bug bounty programs. All complex systems have "bugs"—imperfections unintentionally written within the software's code. Sometimes these bugs create vulnerabilities, which could be exploited by an intruder to gain access to confidential data. Security teams across the industry, including those at Uber, invest heavily in preventing and identifying as many of these bugs as we can before code is updated in our products. However, due to the evolving nature of software, programmers continuously update code by augmenting, rewriting, and overwriting their prior work. That process inevitably results in unexpected errors and vulnerabilities. To help mitigate this reality, bug bounty programs allow companies to access additional skilled individuals to augment our in-house engineers. This outside perspective is also valuable in providing a fresh set of eyes and new ways of thinking to help our security teams address various challenges with innovative solutions.

Typically, a bug bounty program is an invitation for outside experts (commonly referred to as "researchers") to search voluntarily for vulnerabilities and report them to the company or government agency that is the sponsor of the particular bug bounty program. This is supposed to be done pursuant to specific guidelines, as well as defined parameters regarding the types of systems that should be searched. For example, Uber posts a "treasure map" online to tell our researchers where to look for bugs in our systems. It points our researchers to the systems we care the most about.

Companies typically offer rewards, or "bounties," in recognition of the work performed by the researchers. Monetary bounties vary in size, from hundreds of dollars to hundreds of thousands of dollars, depending on the severity of the bug. Companies may also offer physical items, such as branded apparel, commemorating bugs that are found, as a non-monetary reward for the researcher. "Street cred" and public recognition also go a long way to motivate researchers, so many companies publish information about the most impressive bugs found.

Not surprisingly, the security benefits of bug bounty programs have motivated many major technology companies, including Uber, Google, Facebook, Microsoft, and others, to implement bug bounty programs. Moreover, the U.S. Government also has recognized the value of bug bounty programs to protect its sensitive information technology systems. For example, the U.S. Department of Defense has bug bounty programs such as "Hack the Pentagon" and "Hack the Air Force," which the Department has operated with great success. In addition, last July, the Computer Crime and Intellectual Property Section of the U.S. Department of Justice issued *A Framework for a Vulnerability Disclosure Program for Online Systems,* which provides helpful guidance on how to design and operate a bug bounty program.

In 2015, when I joined the company, one of the first things we did to improve security was launch a bug bounty program. This was a private "beta" program and included about two hundred researchers who helped us identify and remediate nearly 100 bugs. Following the success of our beta program, we launched a public bug bounty program in March 2016. Our current program, hosted by HackerOne, offers a combination of public recognition and monetary bounties as incentives for researchers to search our products and websites for potential bugs.

Since its initial launch, this bug bounty program has assisted Uber in resolving more than 800 system vulnerabilities. The program's monetary payout stands at approximately $1.3 million in total. For us, this bug bounty program has been incredibly valuable, achieving very significant improvements in our data security posture for a relatively modest expenditure. I believe many other companies and agencies have had a similar experience with bug bounty programs.

Our bounties typically range from a few hundred dollars to several thousand dollars—depending on the impact and severity of the bug. Given the large number of companies with bug bounty programs, monetary payments can help incentivize bug hunters to focus on Uber's bugs. That is, companies compete for the time and attention of these outside researchers, and relatively modest monetary incentives help ensure that researchers focus their attention on our software. Again, I think many companies and agencies have reached this same view.

The vulnerabilities found by our researchers demonstrate the concrete value of bug bounty programs. As we have publicly shared, one researcher discovered a bug in the SSH authentication system used between different internal services. If exploited, the bug could have allowed escalation of internal privileges. This would have allowed people to access systems they did not have privileges to access. Another researcher who participated in our public bug bounty program found a "remote code execution" bug on one of our websites. This was an important issue because remote code execution gives attackers the ability to run commands on a target computer. In this case, the researcher demonstrated the ability to execute commands on a system within our data center. Potentially, a malicious attacker could have used this vulnerability to access sensitive user data.

Uber's bug bounty program unquestionably has increased the scale and speed at which we are able to identify and eliminate cybersecurity threats. We are constantly refining our tools to prevent the bugs that are found from being written into our code in the first place.

Over the nearly three years we have been running this program, more than 500 researchers have participated. Through our bug bounty program, we can benefit from a vast, diverse, worldwide pool of talent, often beyond our ability to hire.

Of course, operating a bug bounty program is not without its challenges. Security researchers can be an eccentric group, and within this community there are individuals with varying degrees of technical experience and professionalism who engage through bug bounty programs. Researchers sometimes express concern with the amount of the bounty that is paid, believing that their discovery may be worth more than we determine was appropriate, based on our program guidelines. Other times, a researcher may identify a bug that we already know and are working to fix. The researcher sometimes takes issue with not receiving a monetary reward for those already identified bugs. Occasionally, a person may contact the company to report a vulnerability (without exploiting it), completely unaware of our bug bounty program, and make a demand for compensation. We try to work with such persons to submit their report through the bug bounty program in exchange for a fair reward under the program guidelines.

2016 Uber Data Security Incident

The 2016 data security incident unfolded in a way that is entirely different from the typical bug bounty program scenario. On November 14, 2016, Uber's security team received e-mails from an anonymous individual who claimed to have accessed Uber data and demanded a six-figure payment. Uber investigated and determined that the individual and another person working with him had obtained access to certain archived copies of Uber databases and files located on Uber's private cloud data storage environment on Amazon Web Services ("AWS"). In line with standard protocol, Uber assembled an incident response team. This team included technical experts whom I directed, and we worked quickly to determine the means of access, shut down the compromised credential, and take various steps to secure our systems against a further attack. To the best of Uber's knowledge, the intruders' access began on October 13, 2016, and there was no further access by the intruders after November 15, 2016.

For the Subcommittee's information, I would like to explain in greater detail how Uber responded to this security incident. As with any security incident, the first

step was to validate the claims that the intruder had made. Very often these situations are hoaxes. The Uber security team requested data from the intruder, which he provided, and then confirmed that the data were Uber's. With that validation, we initiated an incident response procedure. Incident response to any data incident is an orchestrated affair. The first steps involve fast, intense work with limited information and a very short time to eliminate the threat. We set up a command center where members of the team could work in parallel and discuss issues in real time.

The overall effort was led by our former Chief Security Officer, Joe Sullivan, to whom I reported. I led the technical work to identify how the intrusion occurred and remove the vulnerability. Joe Sullivan and others led what we call "attribution"—the process of identifying the intruders.

During the technical effort, we immediately began the process of determining where the data at issue resided and how the intruder gained access. Within 24 hours, we determined that the data came from back-up files stored in an AWS S3 bucket. S3 stands for "simple storage service."

The next step of the investigation for my team was to determine how the intruder gained access to the AWS S3 bucket, which requires access credentials. We learned that the intruder found the credential contained within code on a private repository for Uber engineers on GitHub, which is a third party site that allows people to collaborate on code. We immediately took steps to implement multifactor authentication for GitHub and rotated the AWS credential used by the intruder. Despite the complexity of the issue and the limited information with which we started, we were able to lock down the point of entry within 24 hours.

Subsequently, we did a thorough review of our GitHub repositories. My technical team initiated the process of removing additional code from GitHub that could be considered sensitive, and confirming rotation of keys. We ceased using GitHub except for items like open source code. The incident response team also worked to identify the type of data downloaded to assess the risk.

In addition to the technical response, another team worked on attribution. Although I was not directly involved, I understand that the attribution team used various methods, including forensics, to gather further information on the intruders. This was a challenging endeavor because the intruders were extremely adept at covering their tracks.

Ultimately, the attribution team ascertained the real identity of both the original individual who contacted the company, and the second person working with him. I understand that the original individual was located in Canada, and that his partner, who actually obtained the data, was in Florida. I further understand that the attribution team made contact with both individuals and received assurances that the data had been destroyed.

As you know, Uber paid the intruders $100,000 through HackerOne and our bug bounty program. Our primary goal in paying the intruders was to protect our consumers' data. This was not done in a way that is consistent with the way our bounty program normally operates, however. In my view, the key distinction regarding this incident is that the intruders not only found a weakness, they also exploited the vulnerability in a malicious fashion to access and download data.

In 2017, after learning about the incident, new company leadership at Uber asked an independent cybersecurity firm, Mandiant, to conduct a thorough analysis of the data at issue. Mandiant's analysis showed that the data included information pertaining to approximately 57 million users worldwide, including approximately 25 million users in the United States. Of these, approximately 4.1 million users in the United States were drivers. For nearly all users, the downloaded files included names, e-mail addresses and phone numbers. In some cases, the information also included information collected from or created about users by Uber, such as Uber user IDs, certain one-time locational information (*e.g.,* the latitude and longitude corresponding to the location where the user first signed up for the Uber service), user tokens, and passwords encrypted using hashing and salting techniques. Of the driver accounts, approximately 600,000 thousand included driver's license numbers.

In their independent analysis, Mandiant found *no* indication that trip location history, credit card numbers, bank account numbers, Social Security numbers, or dates of birth were compromised.

Lessons Learned and Data Security Enhancements at Uber

While the circumstances surrounding the 2016 security incident remain under investigation by the company and multiple regulators, and I am not privy to the details of those ongoing investigations, there are a number of lessons learned that I would like to highlight today.

First, I would like to echo statements made by new leadership, and state publicly that it was wrong not to disclose the breach earlier. The breach should have been disclosed in a timely manner. The company is taking steps to ensure that an incident like this does not happen again, with personnel changes and additional remedial actions. We are working to make transparency and honesty core values of our company. I would add that this is a change that I personally am gratified to see and wholeheartedly support.

Although we regret that we did not publicly report the incident in 2016, we did at that time take numerous steps internally to improve our security posture in response to the incident. As I noted previously, we immediately instituted multifactor authentication on Github. We then subsequently ceased using GitHub except for items like open source code. As to AWS, we were already using multifactor authentication for individual access accounts—which these intruders did not compromise. After the incident we expanded the use of multifactor authentication protocols for AWS service accounts using techniques such as IP restrictions, commonly referred to as "white listing." We have also taken other steps to enhance security for AWS data storage, such as refining Identity & Assessment Management permissions, improving our ability to authenticate someone before granting access to these systems and to confirm whether they are authorized to access them. We also added auto-expiring credentials to protect further against attacks using exposed, lost, or shared credentials. We continue to look to Amazon's evolving best practices and guidance to protect our AWS system.

We recognize that the bug bounty program is not an appropriate vehicle for dealing with intruders who seek to extort funds from the company. The approach that these intruders took was separate and distinct from those of the researchers in the security community for whom bug bounty programs are designed. While the use of the bug bounty program assisted in the effort to gain attribution and, ultimately, assurances that our users' data were secure, at the end of the day, these intruders were fundamentally different from legitimate bug bounty recipients.

Going forward, Uber is revisiting its incident response approach in circumstances such as these. We have hired Matt Olsen, a former general counsel of the National Security Agency and director of the National Counterterrorism Center, to help structure the security team and guide new processes going forward. I have already seen some of these changes take place, such as more stakeholders involved in the decision-making process for how to handle security incidents, and informing law enforcement of potential security incidents right away.

I would like to conclude by stating that we strongly support a unified, national approach to data security and breach standards. We are proactively engaged in the many conversations in both the technical and policy communities to help identify what the critical components of federal data breach legislation should be, and are pleased to see this robust conversation taking place with various Members of Congress and your staff. We welcome the opportunity to be at the table to help all stakeholders understand the best practices.

* * *

Thank you again for the opportunity to appear and testify today. I would be happy to answer your questions.

Senator MORAN. Thank you.

Mr. Mickos.

STATEMENT OF MARTEN G. MICKOS, CEO, HACKERONE

Mr. MICKOS. Chairman Moran, Senator Blumenthal, Ranking Member Nelson, and members of the Subcommittee, thank you for inviting me to testify today.

I look forward to providing you with my perspective on data security and bug bounty programs.

Mr. Chairman, a brief note. As I have informed your staff, there are legal proceedings with respect to the Uber incident. We are cooperating fully and eagerly in those proceedings. As a result of these proceedings, however, I will unfortunately not be able to discuss many aspects of that incident.

I am the Chief Executive Officer of HackerOne, the world's leading provider of hacker-powered security. HackerOne operates bug bounty programs that connect companies and governments with the world's best white hat hackers to find and fix vulnerabilities before malicious actors exploit them.

It all starts with the vulnerability disclosure program, which is essentially a neighborhood watch for software. When an entity decides to offer financial rewards to finders of vulnerabilities, the vulnerability disclosure program becomes a bug bounty program.

Such programs are useful for organizations large and small, in the private and in the public sector. Examples include: Adobe Systems, GSA, General Motors, Qualcomm, Starbucks, United Airlines, and many more. Some of them run their own homegrown programs, others will run their program on a platform, such as HackerOne.

The nature of HackerOne's business is preventative. We are not in the incident response business. We are in the data breach prevention business. Through HackerOne's service alone, over 63,000 vulnerabilities have been found and fixed. The average bounty is approximately $500 and the current maximum bounty listed on HackerOne is $250,000. No other method has been shown to produce similar results with such favorable economics.

Organizations signing up with HackerOne typically start with an invitation-only program. Later, the program can be made public, in which case any hacker is allowed to submit reports.

It is the customer who decides on the bounties. To receive any form of payment by a HackerOne, the hacker must submit identifying information and the appropriate tax forms.

HackerOne is committed to compliance with all relevant rules and regulations. Additionally, we have internal guidelines and specific terms and conditions that apply to hackers and to customers, respectively.

The Federal Government is an innovator in this area. The U.S. Department of Defense and HackerOne pioneered the first Federal Government Bug Bounty Program called "Hack the Pentagon." Since the program's inception, more than 3,600 security vulnerabilities have been safely resolved in critical DoD assets.

FTC, NTIA, FDA, NHTSA, and the Department of Justice have declared vulnerability disclosure programs as cyber security best practice. These agencies recognized the critical role that hackers play in securing technology and protecting consumers.

For instance, in July 2017, the Department of Justice published a framework for vulnerability disclosure program for online systems to provide guidance to entities on setting up a program.

Our goal must be an internet that enables privacy and protects consumers. This is not achievable without ethical hackers taking an active role in safeguarding our collective security, and that in turn requires a safe legal environment encouraging all individuals to come forward with vulnerability information, no matter the circumstances.

I would like to offer three recommendations. First, I encourage you to support CFAA reform that removes criminal penalties on actions that do no harm, protecting individuals that act in good faith to identify and report potential vulnerabilities.

Second, I encourage you to support a harmonized and unambiguous breach notification law governing all consumer-facing entities. Those who in good faith operate or participate in a vulnerability disclosure policy should not be legally exposed.

Third, Congress should encourage data security best practices that require all companies responsible for safeguarding consumer data to implement a vulnerability disclosure policy.

In summary, Mr. Chairman, we need hackers. Ethical hacking may be the only force that can stop criminal hacking. Hundreds of thousands of security vulnerabilities have already been found and remediated. Hacker-powered security does not only protect consumers, it also creates opportunity for aspiring hackers across the country.

With this, thank you for the opportunity to testify on this important issue, and I look forward to any questions you may have.

[The prepared statement of Mr. Mickos follows:]

PREPARED STATEMENT OF MARTEN G. MICKOS, CHIEF EXECUTIVE OFFICER, HACKERONE

Introduction

Chairman Moran, Ranking Member Blumenthal, and Members of the Subcommittee, thank you for inviting me to testify today. I look forward to providing you with my perspective on Data Security and Bug Bounty Programs.

I am Chief Executive Officer of San Francisco-based HackerOne, the world's leading provider of hacker-powered security. I have spent my entire 30-year career in software, including as Senior Vice President at both Hewlett-Packard and Sun Microsystems, and prior to that as CEO of MySQL. In addition, I served on the Board of Directors of Nokia Corporation.

HackerOne operates bug bounty programs that connect companies and governments with the best white hat hackers in the world to find and fix vulnerabilities before malicious actors exploit them. As of January 2018, over 160,000 white hat hackers have registered with HackerOne to defend customers, among them the United States Department of Defense, removing over 60,000 vulnerabilities and preventing an untold number of breaches in the process.

The Threat of Weak Cybersecurity

Today's cybersecurity practices are severely outdated in contrast to the cyber threats that society faces. When exploited for criminal purposes, even just one single and relatively unremarkable security vulnerability can create havoc, as the Equifax data breach [1] grossly reminded us of in 2017.

Unfortunately it is only a question of time before cybercrime causes physical damage to structures or, worse, physical harm to humans. Citizens in general and consumers in particular are exposed to risks that they cannot possibly deal with themselves. Privacy is threatened. Consumer protection against faulty and vulnerable software-based products is presently inadequate.

The economic repercussions are enormous, and we are only now starting to see the true costs of lax cyber hygiene. When data breaches occur, corporations lose millions of dollars. These costs are often passed along to consumers who additionally face unquantifiable burdens associated with the breaches, including compromise of privacy.

It is an unfortunate fact that in the digital realm, society is currently failing to provide its citizens with what societies were established for: safety and security.

Hacker-Powered Security Offers a Solution

Whatever protections and defenses we build into our digital assets—and we should build a lot of them—there is one practice that covers every possible cause of cyber breach. There is an "immune system" [2] that will approach the digital assets from the same direction as adversaries and criminals do—from the outside. There is a mechanism that at scale has the opportunity to ultimately detect every hole,

[1] *https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do*
[2] *https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system*

every weakness and every security vulnerability in a system or product built by humans.

This practice is often called "Hacker-Powered Security." It is a mechanism that turns the asymmetry that favors the attacker into an asymmetry that favors the collaborating defenders. It is a collective effort that relentlessly looks for more vulnerabilities. Its outstanding success metrics are a result of stochastic probability: the more attempts there are at finding vulnerabilities, the higher the likelihood that these will be found. Over time the result improves asymptotically towards 100 percent.

Hacker-powered security is a model that invites external and independent security researchers and ethical hackers—we will here simply call them "hackers"—to hunt for vulnerabilities in computerized systems. Today there are over one hundred thousand white hat hackers in the world. These are individual experts who have signed up to help corporations and organizations to detect and fix their security weaknesses. These hackers are motivated by the challenge, by the opportunity to do good and by peer recognition. They are rewarded for their finds with bounties. They are bug bounty hunters.

How Hacker-Powered Security Works

Hacker-Powered Security covers any cybersecurity-enhancing services and automations that are partially or wholly produced by independently operating security experts outside the company or organization in question.

The most fundamental function of hacker-powered security is a Vulnerability Disclosure Program, also called Responsible Disclosure or Coordinated Vulnerability Disclosure.

A vulnerability disclosure program is essentially a neighborhood watch for software. The motto is "If you see something, say something." Concretely, if and when an ethical hacker finds a security vulnerability in and company or government organization's website or mobile app or other computer system, this person will be invited to disclose the vulnerability found to the system's owner.

Most human beings are ready to help their neighbor, so the impetus for vulnerability disclosure is enormous. Issues of legality and trust, however, make vulnerability disclosure more complicated than a regular neighborhood watch. To solve this issue, leading companies have created their own policy frameworks for the disclosure of vulnerabilities to them, and others turn to companies such as HackerOne to organize and coordinate such programs.

When an entity decides to offer financial rewards to finders of vulnerabilities, the vulnerability disclosure program is called a Bug Bounty Program. Bug bounty programs have existed at least since 1983.[3] The practice was perfected by Google, Facebook and Microsoft over the past half-dozen years. Around the same time, companies such as HackerOne emerged for the purpose of bringing this powerful method within reach of any organization that owns and operates a digital asset (meaning a computer system, a website, a mobile application, an Internet-of-Things device, or some other digital product).

Proven Effectiveness

Hacker-powered security programs have demonstrated their effectiveness compared to other methods for vulnerability detection. Hiring full-time employees or external service or product vendors to test for vulnerabilities is more expensive. Through HackerOne's service alone, over 63,000 security vulnerabilities have been found and fixed. The current maximum bounty listed on HackerOne is $250,000. No other method for validating software or manufactured products that are in use by consumers has been shown to produce similar results at such a favorable economic unit price.

Hacker-powered security is a model that scales. Today there are over 160,000 registered ethical hackers, and over the coming years this number is likely to grow to over a million. This army of hackers will be able to take on the work of the entire digital realm of our society.

Thanks to the diversity and scale of the hacker community, hacker-powered security finds vulnerabilities that automated scanners or permanent penetration testing teams do not find. Existing models are good at finding predictable security vulnerabilities, but even more important is to find the unpredictable ones—the unknown unknowns. Given a large enough hacker community and enough time, such vulnerabilities will be identified.

---

[3] Hunter & Ready ran a campaign in 1983 called "Get a bug if you find a bug", offering a VW beetle as reward for bugs found in their real-time operating system. Netscape launched a bug bounty program in 1995.

Vast and Diverse Clientele

Hacker-powered security emanated over the past decade as a best practice among Silicon Valley tech companies. Today, the model has matured and became applicable to all types of businesses. Any company, corporation, association or public sector agency that develops and deploys software (in whatever form, such as embedded in hardware) can benefit from hacker-powered security.

The vendors providing hacker-powered services have established communities of ethical hackers for whom they keep track of skill profiles and performance metrics. Bug bounty programs may be self-managed by the customer, or fully managed by the vendor. In the latter scenario, customers save both time and money while being presented with valid security vulnerabilities on a continuous basis. In either scenario, it is up to the customer to remediate the vulnerability once found.

Entities that operate such vulnerability disclosure and/or bug bounty programs include: Adobe, AT&T, CERT Coordination Center, U.S. Department of Defense, Dropbox, Facebook, Fiat Chrysler, U.S. General Service Administration, General Motors, GitHub, Google, LendingClub, Microsoft, Nintendo, Panasonic Avionics, Qualcomm, Snapchat, Starbucks, Spotify, Twitter, and United Airlines. Hacker-powered security is useful and accessible for organizations both large and small, technology-focused or not, in the private or public sector. The model is suitable for all entities that develop and deploy software.

Who are the Hackers?

The original experts at the Massachusetts Institute of Technology (MIT) defined themselves as *"one who enjoys the intellectual challenge of creatively overcoming limitations."*

Security experts may be described using a variety of titles including "ethical hacker", "white hat", "security researcher", "bug hunter", and "finder." One title is conspicuously absent: Criminal. Hackers are not criminals. Specifically, bug bounty platforms offer no benefit to someone with criminal intent. On the contrary, HackerOne will record data about every hacker on the platform and only reward actions that follow the rules. For these reasons, criminals go elsewhere.

Hackers are driven by a variety of motivations, many of which altruistic. The security advocacy organization *I Am The Calvary* summarizes these motivations [4] as: *Protect* (make the world a safer place), *Puzzle* (tinker out of curiosity), *Prestige* (seek pride and notability), *Profit* (to earn money), and *Protest/Patriotism* (ideological and principled).

The HackerOne 2018 Hacker Report [5]—a survey of over 1,000 hackers—revealed that profit was only the fourth most common motivation for why hackers do their work. Before that came the desire to learn, be challenged, and have fun. To protect and defend is also a central motivation for hackers. A 2016 study by the National Telecommunications and Information Administration (NTIA) within the Department of Commerce found that only 15 percent of security researchers expect financial compensation in response to a vulnerability disclosure.[6]

Hacker-powered security does not only improve security. The model democratizes opportunity and offers meaningful work to anyone with the inclination and drive to be a useful ethical hacker. Many hackers are young adults. They can do their work from anywhere. The money hackers make is used to support their families, pay for education, and catapult them into successful professional careers. Hacking brings meaning and mandate to enterprising people irrespective of their location. Hacking brings positive societal impact across the Nation.

Case Studies

The U.S. Department of Defense (DoD) and HackerOne pioneered the first Federal government bug bounty program. Since the program's inception, more than 3,600 security vulnerabilities have been safely resolved in DoD critical assets with hacker-powered security. While the majority of the vulnerabilities reported through the DoD vulnerability disclosure policy were without financial compensation, hackers have been awarded hundreds of thousands of dollars in bug bounty payments by DoD.

"Hack the Pentagon" was initially launched as a pilot program under the leadership of Secretary of Defense Ash Carter. This pilot ran from April 18 to May 12, 2016. During that short time more than 250 vetted ethical hacker participants sub-

---

[4] *https://www.iamthecavalry.org/motivations*
[5] *https://www.hackerone.com/sites/default/files/2018–01/2018_Hacker_Report.pdf*
[6] *https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.p*

mitted vulnerability reports. A total of 138 valid vulnerabilities were found and remediated.

"We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks," said Secretary Carter of Hack the Pentagon.[7] "What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference—hackers who want to help keep our people and nation safer."

"It's not a small sum, but if we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us more than $1 million,"[8] Carter said of the $150,000 pilot program.

The Pentagon announced it would continue Hack the Pentagon program and bring this successful model to other agencies.

Hack the Army

The "Hack the Army" Bug Bounty program[9] ran from November to December 2016 with 371 registered, vetted and eligible participants. Of those who participated 25 were government employees including 17 military personnel. Of the 416 vulnerability reports submitted by hackers, 118 were unique, valid and actionable. The first one was filed within 5 minutes of the launch of the program.

While bug bounties are a way for the DoD to tap into private sector talent, sometimes the cybersecurity talent is already within their ranks. One of the researchers that successfully hacked the U.S. Army was an Army Captain presently in school at the Army's Cyber Center of Excellence at Fort Gordon, Georgia. In addition to having a full-time job and family, this officer registered for Hack the Army to get real, operational hands-on training in addition to his extensive schooling.

Hack the Air Force

It took just under one minute for hackers to report the first security vulnerability to the U.S. Air Force. Within the first 24 hours, 70 reports were submitted, 23 of which were valid. During the "Hack the Air Force" bug bounty challenge, 207 valid vulnerabilities were discovered. Nearly 300 vetted individuals had registered to participate in the Hack the Air Force bug bounty challenge and more than 50 earned bounties.

"Adversaries are constantly attempting to attack our websites, so we welcome a second opinion—and in this case, hundreds of second opinions—on the health and security of our online infrastructure,"[10] said Peter Kim, the Air Force Chief Information Security Officer. "By engaging a global army of security researchers, we're better able to assess our vulnerabilities and protect the Air Force's efforts in the skies, on the ground and online."

Two of the Hack the Air Force participants were military personnel opting to help as an act of patriotism despite being ineligible for bounties, and 33 participants came from outside the U.S. Some of the top participating hackers were under 20 years old, including a 17 year-old from Chicago who earned the largest bounty sum for 30 separate discoveries.

The Hack the Air Force bug bounty challenge was so successful that the Air Force ran a second bug bounty challenge—Hack the Air Force 2.0—in December 2017.

Consistency with Existing Laws & Best Practices

Federal regulatory agencies responsible for consumer safety have acknowledged and adopted vulnerability disclosure programs as a cybersecurity best practice. These agencies recognize the critical role that hackers play in securing technology and protecting consumers.

In June 2015, the Federal Trade Commission (FTC) published security guidance for businesses summarizing security best practices from the agency's 50+ data security settlements.[11] One common cause for complaint against an organization's security practices was the lack of a vulnerability disclosure process. For example: "FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant

---

[7] *https://www.defense.gov/News/News-Releases/News-Release-View/Article/802929/defense-secretary-ash-carter-releases-hack-the-pentagon-results/*

[8] *https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/*

[9] *https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In*

[10] *http://www.af.mil/News/Article-Display/Article/1274518/hack-the-air-force-results-released/*

[11] *https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business#current*

that the vulnerabilities found their way onto even more devices across multiple operating system versions."

In later comments made by the FTC to the NTIA Safety Working Group,[12] the commission reaffirmed the importance of this practice: "[FTC] staff highlighted the important role that vulnerability reports play in ensuring product security, and recommended that businesses implement reasonable vulnerability disclosure processes to facilitate communication with the research community."

In October 2016, the National Highway Traffic Safety Administration (NHTSA) published *Cybersecurity Best Practices for Modern Vehicles.*[13] It states: "Automotive industry members should consider creating their own vulnerability reporting/disclosure policies, or adopting policies used in other sectors or in technical standards. Such policies would provide any external cybersecurity researcher with guidance on how to disclose vulnerabilities to organizations that manufacture and design vehicle systems." Major automakers, including General Motors[14] and Tesla,[15] have adopted policies for encouraging hackers to identify and disclose vulnerabilities in their connected automobiles.

In December 2016, the Food and Drug Administration published *Postmarket Management of Cybersecurity in Medical Devices*,[16] noting that ". . .cybersecurity information may originate from an array of sources including independent security researchers.." and described "Adopting a coordinated vulnerability disclosure policy and practice" as a critical component of any medical device manufacturer cybersecurity program.

In July 2017, the Department of Justice (DoJ) Criminal Division's Cybersecurity Unit published *"A Framework for a Vulnerability Disclosure Program".*[17] The DoJ observes "[organizations are] adopting vulnerability disclosure programs to improve their ability to detect security issues on their networks that could lead to the compromise of sensitive data" and goes on to provide guidance for operating these programs in a manner consistent with existing cybercrime laws.

In October 2017, deputy attorney general Rod Rosenstein made this public statement:[18] "All companies should consider promulgating a vulnerability disclosure policy, that is, a public invitation for white hat security researchers to report vulnerabilities. The U.S. Department of Defense runs such a program. It has been very successful in finding and solving problems before they turn into crises."

These Federal agencies have recognized the critical role that ethical hackers play in enabling public and private sector organizations to provide secure services that are resilient to cybersecurity vulnerabilities.

Conclusion and recommendation

We need hackers. Our goal must be an Internet that enables privacy and protects consumers. This is not achievable without ethical hackers taking an active role in safeguarding our collective security.

Hackers are truly the immune system of the internet. They are a positive power in society. We must enable and encourage them to make their best security contributions. This requires a safe legal environment encouraging all individuals to come forward with vulnerability information, no matter the circumstances.

I provide you with the following recommendations:

First, the Computer Fraud and Abuse Act (CFAA), enacted in 1984, contains vague wording that has not kept pace with the proliferation of the internet. The act is in need of modernization. I encourage the members of the committee to support CFAA reform[19] to remove imposed criminal penalties on actions that do no harm to consumers. Individuals that act in good faith to identify and report potential vulnerabilities should not be legally exposed.

Second, the patchwork of breach notification laws enacted primarily at the state level may create uncertainty and perverse incentives for those who safeguard consumer data. I encourage this subcommittee to support a harmonized and unambiguous breach notification law governing all U.S. companies and consumers. It is im-

---

[12] *https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf*

[13] *https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf*

[14] *https://hackerone.com/gm*

[15] *https://www.tesla.com/about/security*

[16] *https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf*

[17] *https://www.justice.gov/criminal-ccips/page/file/983996/download*

[18] *https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber-security-summit*

[19] *https://www.eff.org/document/letter-def-con-cfaa-reform*

portant that such a law provide clarity on the definition of a data breach to ensure that those who operate or participate in a good faith vulnerability disclosure policy are not legally exposed.

Third, I repeat the words of numerous experts that a ubiquitous "See something, Say something" practice for vulnerabilities is a vital and critical step towards improving cybersecurity for consumers. The absence of a formal channel to receive vulnerability reports reduces a vendor's security posture and introduces unnecessary risk. Corporations should welcome input from external parties regarding potential security vulnerabilities and Congress should encourage that behavior.

As Jeff Massimilla, Vice President for Vehicle Safety and Product Cybersecurity at General Motors, stated: "To improve the security of their connected systems, every corporation should have a vulnerability disclosure policy that allows them to receive security submissions from the outside world." [20]

Hacker-powered security has matured as a model to be ready to help society solve one of its most pressing problems: cyber threats.

Pioneering entities have perfected the practice of hacker-powered security. Hundreds of thousands of security vulnerabilities have already been found and remediated. The vast community of hackers stands ready. The hackers are not asking what society can do for them. They are asking what they can do for society. Ethical hacking may be the only force that can stop criminal hacking. The asymmetry of digital threats can be turned around with pooled defense. Together we hit harder against cybercrime.

Thank you for the opportunity to testify on this important issue.

Senator MORAN. Thank you for joining us.

Ms. Moussouris.

STATEMENT OF KATIE MOUSSOURIS, FOUNDER AND CEO, LUTA SECURITY

Ms. MOUSSOURIS. Chairman Moran, Ranking Member Blumenthal, and distinguished members of the Committee, thank you for the opportunity to testify at this hearing on behalf of Luta Security and the security research community.

We commend the Committee for holding this open hearing to help understand, clarify, and differentiate between defensive security research and vulnerability disclosure activities which may or may not include bug bounties versus internet-enabled crimes which may include extortion for unauthorized access to consumer data.

I'm the Founder and CEO of Luta Security, working with governments and complex organizations on multi-party supply chain vulnerability coordination to create mature, robust, and sustainable vulnerability coordination and disclosure programs.

We base these programs on the Industry International Standards, ISO 29147, Vulnerability Disclosure, and ISO 30111, Vulnerability Handling Processes, and our own Vulnerability Coordination Maturity Model.

I am the co-author and co-editor of these international standards, was Co-chair of the NTIA's Multi-stakeholder Vulnerability Disclosure Working Group Subcommittee of Multiparty Vulnerability Coordination, and I have over 20 years of professional, technical, and strategic work in technology and information security as a former penetration tester or ethical hacker for hire at the company called @stake to creating Microsoft vulnerability research, the first Microsoft bug bounties, and advising the U.S. Department of Defense for several years resulting in the launch of the "Hack the Pentagon" Program.

---

[20] *https://www.cnet.com/roadshow/news/general-motors-cybersecurity/*

But today, I'm here as a witness to talk about the defense market for bugs, the role of bug bounties and other security research, and the role of the defensive ecosystem to shape these new markets.

When I was a teenager learning to hack in the late 1980s, there was no broadly recognized and accessible defense market for hacking skills. There were no online banks or e-commerce sites to hire us to test their internet-facing systems for holes, and there certainly weren't any bug bounty programs.

Even the U.S. Government had only a few years earlier become aware of threats to national security across the burgeoning early internet through Hollywood films, such as *War Games.*

Only in the past five to eight years have we seen any major acceptance by governments and companies working cooperatively and openly with hackers. However, there is still a great fear among many organizations that opening a front door for hackers to report security holes will cause damage from disruption of operations, intellectual property theft, fraud, reputational damage, and, of course, data breaches.

In 2015, 94 percent of the Forbes Global 2000 had no published way to report a security hold to them. If you saw something, it was very difficult and risky to say something.

So while the Computer Fraud and Abuse Act hasn't materially changed over the past 34 years to grant security researchers safe harbor, in July 2017, the Department of Justice issued "Framework for Vulnerability Disclosure Program for Online Systems" and this guide is meant as a way to help organizations think through important scoping issues around protected classes of data and systems when creating vulnerability disclosure programs with or without cash incentives.

The main premises are: decide whether sensitive systems and data are in scope for discovery; encourage the use of test accounts whenever possible to avoid the unnecessary compromise of other users' privacy and data without their permission; make it clear that only the minimum necessary proof is required to prove that a vulnerability exists and no further access or exploitation past that point is authorized.

Further, define how any deliberately or accidentally, because "hackidents" happen, accidentally accessed private data should be stored and transmitted and specify the manner in which the proof of the hack is conveyed, perhaps using a screen capture so as to not further transmit unauthorized accessed data.

So this is to protect both the well-intentioned researchers from ambiguity and accidental overstepping as well as to protect consumers whose data may be subject to access.

And, finally, as a creator and advisor to some of the major new bug bounty programs in the past several years, I want to point out that the ecosystem for reward bug hunting is skewing the markets toward more bug hunters but not necessarily more bug fixers.

This imbalance that's being created in these markets may very well shift the ecosystem toward rewarding more data theft than bug hunting. Already we are facing a global shortage of talent in cyber security and an overall workforce creation is necessary in defense.

We have got over 350,000 unfilled cyber security positions in the United States that are open and, according to a 2016 study, none of the top 10 U.S. computer science programs required a cyber security course for graduation and three of the top 10 universities don't even offer an elective course in cyber security.

The defense market for bugs that we are creating needs to be focused. Markets are not inevitable. They are actively created. If I were to recommend three practices, it would be funding for increased education in security to be set for all grades, setting forth requirements that all college majors in computer science understand secure coding and organizational cyber risk management, and a reflection on fewer "hack the X" bills being introduced without proper assessment of sustainable defensive capabilities in each government agency considering a bug bounty.

Thank you for the opportunity of testifying. I welcome your questions and comments.

[The prepared statement of Ms. Moussouris follows:]

STATEMENT OF KATIE MOUSSOURIS FOR THE HEARING ENTITLED, "DATA SECURITY AND BUG BOUNTY PROGRAMS: LESSONS LEARNED FROM THE UBER BREACH AND SECURITY RESEARCHERS" FOR THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION'S SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY [1] ON TUESDAY, FEBRUARY 6, 2018

Chairman Moran, Ranking Member Blumenthal, and distinguished members of the Committee, thank you for the opportunity to testify at this hearing on behalf of Luta Security and the security research community.

We commend the Committee for holding this open hearing to help understand, clarify, and differentiate between defensive security research and vulnerability disclosure activities, which may or may not include bug bounties, versus Internet-enabled crimes, which may include extortion for unauthorized access to consumer data.

I am the founder and CEO of Luta Security, working with governments and complex organizations on multi-party supply chain vulnerability coordination to create mature, robust, sustainable vulnerability coordination and disclosure programs. We base these programs on the industry international standards ISO/IEC 29147 Vulnerability disclosure,[2] ISO/IEC 30111 Vulnerability handling processes,[3] and our Vulnerability Coordination Maturity Model.

I am the co-author & co-editor of these international standards, was co-chair of the NTIA's multi-stakeholder vulnerability disclosure working group subcommittee of multi-party vulnerability coordination,[4] with over 20 years of professional technical and strategic work in technology and information security, as a former penetration tester at @stake,[5] to creating Microsoft Vulnerability Research, the first Microsoft bug bounties, and advising the U.S. Department of Defense for years, resulting in the launch of the Hack-the-Pentagon program. I am also one of two private industry official delegates of the U.S. technical experts working group to renegotiate the Wassenaar Arrangement,[6] successfully helping clarify exemptions for vulnerability disclosure and incident response in export controls.[7] I served as an expert witness for European Parliament's consideration of dual-use export control reform in the context of vulnerability disclosure and bug bounty programs.[8]

---

[1] *https://www.commerce.senate.gov/public/index.cfm/2018/2/data-security-and-bug-bounty-programs-lessons-learned-from-the-uber-breach-and-security-researchers*

[2] *http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147*

[3] *https://www.iso.org/standard/53231.html*

[4] *https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf*

[5] *https://en.wikipedia.org/wiki/@stake*

[6] *https://langevin.house.gov/press-release/langevin-statement-wassenaar-arrangement-plenary-session*

[7] *http://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global*

[8] *https://www.youtube.com/watch?v=kDJxAm-AVNA&feature=youtu.be*

Today, I'm here as a witness to talk about the defense market for bugs, the role of bug bounties and other security research, and the role of the defensive ecosystem to shape these new markets.

When I was a teen learning to hack in the late '80s, there was no broadly-recognized and accessible defensive market for hacking skills, no online banks or e-commerce sites to hire us to test their Internet-facing systems for holes, no bug bounty programs, and even the United States government had only a few years earlier become aware of threats to national security across the burgeoning early Internet—through Hollywood films such as War Games.

This awareness of the power of hackers had prompted not job offers or viable legal career paths, but legislation that made hacking a criminal offense.[9] This law not only gave prosecutors the necessary legal tools to go after nation state actors and criminals, but to this day has caused a chilling effect on security research for defensive purposes. This chilling effect on researchers has also been reflected in the reluctance of governments and organizations to engage with hackers, further complicated by recent data breaches under the mis-applied term "bug bounty".

Only in the past 5 to 8 years have we seen any major acceptance by governments and companies working cooperatively and openly with hackers. However, there is still a great fear among many organizations that opening a front door for hackers to report security holes will cause damage from disruption of operations, intellectual property theft, fraud, reputational damage, and data breaches.

In 2015, 94 percent of the Forbes Global 2000 had no published way to report a security hole to them. If you saw something, it was difficult to say something. It was even a risk to your freedom, if the organization chose to pursue legal action against you under the Computer Fraud and Abuse Act (CFAA).

While the CFAA hasn't materially changed over the past 34 years to grant security researchers safe harbor for helping to point out security bugs, in July of 2017, the Department of Justice issued "A Framework for a Vulnerability Disclosure Program for Online Systems."[10] This guide is meant as a way to help organizations think through important scoping issues around protected classes of data and systems when creating vulnerability disclosure programs, with or without cash incentives or bug bounties.

The main premises to help create robust vulnerability disclosure or bug bounty programs are straightforward in the DoJ framework, with a summary of the key aspects as follows:

1. Decide whether sensitive systems and data are in scope for discovery and reporting by external helpful hackers.
2. Encourage the use of test accounts whenever possible to avoid the unnecessary compromise of other users' privacy and data without their permission.
3. Make it clear that only the minimum necessary proof is required to prove that a vulnerability exists, and that no further access or exploitation past that point is authorized.
4. Further define how any deliberately or accidentally accessed private data should be stored and transmitted.
5. Specify the manner in which proof of the hack is conveyed, perhaps using a screen capture to avoid further transmitting the protected data.
6. Decide whether to include the requirement to destroy any copies of data once the report is delivered.

To protect both well-intentioned researchers from ambiguity and accidental overstepping the intended scope, as well as to protect consumers whose data may be subject to access, transmission, and storage without their consent, it is important to define these parameters as clearly as possible. This applies in vulnerability disclosure programs as well as bug bounties.

Finally, as a creator and advisor of some of the major new bug bounty programs in the past several years, I want to point out that the ecosystem for rewarding bug hunting is skewing the markets toward more bug hunters, but not necessarily more bug fixers. This imbalance that is being created in these markets may very well shift the ecosystem towards rewarding more data theft than bug hunting.

There is a difference between paying $10,000 for a bug and paying $100,000 for a breach. If the legal market for bugs becomes muddied with extortion payments that are exponentially higher, we will be building the wrong kind of market, and

---

[9] *https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html*

[10] *https://www.justice.gov/criminal-ccips/page/file/983996/download*

consumers will be the victims instead of the beneficiaries of enhanced work with hackers.

Already, we are facing a global shortage of talent in cyber security, and while more legal ways to report bugs is good, the creation of an overall defense workforce is necessary, in the United States and worldwide.

"In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings. . ."

"With more than 200,000 open cybersecurity jobs in 2015 in the U.S. alone and the number of threat surfaces exponentially increasing, there's a growing skills gap between the bad actors and the good guys. One way to close the gap is through automation, but we also need to train developers, at the very earliest stage of their education, to bake security into all new code. It's not good enough to tack cybersecurity on as an afterthought anymore. This is especially true as more smart devices become Internet accessible and therefore potential avenues for threats."

According to a 2016 study, "none of the top 10 U.S. computer science programs required a cybersecurity course for graduation, and 3 of the top 10 university programs don't even offer an elective course in cybersecurity." [11]

Much like in Star Wars, The Force for finding vulnerabilities has a dark side as well as a light side, but they are two sides of the same coin, representing indistinguishable skill sets. We are creating more of an imbalance in The Force, weighted against defenders.

As a visiting scholar with MIT Sloan School helping to study the vulnerability economy and exploit markets, I helped clarify the differences in the offense and defense markets for bugs. The offense market is characterized by nation states and criminals buying bugs and exploits at high prices to keep them from being fixed as long as possible to prolong their use in attacks.

The defense market is typically paying lower amounts than the offense market, but doesn't traditionally require the bug hunter to stay silent about their find, once it is fixed, providing the finder with recognition and further opportunities for their career in other ways.

The defense market for bugs cannot compete directly with the offense market on price.

Very quickly, we would run out of willing software developers and testers, and the markets are already taking that direction in the way that bug bounties are being used today. Bug bounty hunters worldwide are on average able to make more than being a software developer in many countries. Perverse incentives include overpaying for bugs on the defense market, as well as the rewarding of data theft with much higher prices than an honest bug hunter would get for adhering to the rules.

The entire defensive bug hunting ecosystem has a responsibility to help uphold the law & guide the creation of programs that will not breach ethical or legal standards. We have a responsibility to the current and next generation of hackers to demonstrate best practices in bug bounties as well as the broader vulnerability disclosure picture.

"Focusing on the labor market opens new productive avenues for conversation and future research: It suggests linkages between research on vulnerability markets and a larger body of work rooted in the tradition of economic sociology. These efforts consider markets not only or, at times, not even primarily—as engines of efficient resource allocation, but move to address pressing descriptive questions related to the contingent and historical specificity of the construction of markets. Markets are not inevitable. They are always actively created." [12]

If Congress were to act to help clarify the role of defensive security research, and encourage the growth of the defense market for bugs, as well as the United States labor workforce in cybersecurity defender roles, I would ask that:

1. Funding for increased education in security be set for all grades (K–12), to begin finding early security talent and recruiting for defense
2. Setting forth requirements that all college majors in computer science understand secure coding and organizational cyber risk management

---

[11] *https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/*

[12] Ryan Ellis, Keman Huang, Michael Siegel, Katie Moussouris, and James Houghton. "Fixing a Hole: The Labor Market for Bugs." New Solutions for Cybersecurity. Howard Shrobe, David L. Shrier, and Alex Pentland, eds. Cambridge: MIT Press. In Press. ISBN: 9780262535373 *https://mitpress.mit.edu/books/new-solutions-cybersecurity*

3. Fewer "Hack the x" bills be introduced without proper assessment of sustainable defensive capabilities in each government agency considering launching a bug bounty.

Again, I'd like to thank you for the opportunity of testifying today. I welcome your questions and comments.

Senator MORAN. Thank you for your testimony.

Mr. Brookman.

STATEMENT OF JUSTIN BROOKMAN, DIRECTOR. PRIVACY AND TECHNOLOGY POLICY, CONSUMERS UNION

Mr. BROOKMAN. Chairman Moran, Members of the Subcommittee, thank you very much for the opportunity to testify here today.

I am here today on behalf of Consumers Union, the advocacy division of *Consumer Reports.* We are the world's largest independent testing organization and we use our ratings content and advocacy to create a fair, safer, and healthier world.

Let me start out by saying the Consumers Union is a strong proponent of bug bounty programs. We believe they play a crucial role in a data security ecosystem that has failed consumers far too often.

The 2016 Uber incident, however, highlights the practices are still developing in this area and we don't always have clear expectations about how these programs should work.

While bug bounty programs are one useful tool in maintaining reasonable security, they are not a magic bullet. Ultimately, in order to fix the poor state of modern security, incentives need to change and that is why we urge Congress to update consumer protection laws to establish reasonable data security requirements and to hold companies accountable for bad practices, and this premise that poor data security practices are widespread is, I hope, not controversial.

We've seen a never-ending torrent of major data breaches punctuated by the exposure of a 145 million social security numbers in last year's Equifax breach. We are connecting more and more smart devices to the internet but they're not always developed with security in mind. Many never get security updates or even have the ability to get updated.

Bug bounty programs represent an innovative approach to data security by leveraging a diverse third-party ecosystem to identify vulnerabilities before they can be taken advantage of by malicious actors.

Last year, *Consumer Reports* released a document that we called The Digital Standard. It's an open-sourced collaboration designed to articulate best practices in privacy and security and related values, such as repairability and interoperability, and in this document, we specifically identify having a bug bounty program as an indicator of good security practices at the company.

Moreover, we identified a commitment not to pursue legal action against security researchers as another indicator of good security practices, the rationale being that this provides a strong disincentive certainly for outsiders to try to improve any particular company's practices but also to security research more generally.

The 2016 Uber incident raises challenging questions about how best to manage bug bounty programs. While I think Uber had a duty to notify its driver's license numbers had been compromised, the case highlights the potential tension between breach notification laws and bug bounty programs and raises other questions.

When should discovery of vulnerability by a third party trigger breach notification to consumers? How can researchers test for bugs without ever touching consumer data? When, if ever, should bounties be negotiable?

And we certainly have concerns about the use of non-disclosure agreements to prohibit discussion of vulnerability, even after it had been remediated.

These are just some of the important questions raised by the case and I applaud the Committee for holding this hearing to explore these and other issues.

Bug bounty programs should and will continue to play an important role in improving data security but they're just one piece. Fundamentally, companies need to have a legal responsibility to use reasonable security to protect personal information and that is why Congress needs to act to update legal protections for consumers to reflect the extremely real threat posed by poor data security.

There are a few things I think Congress can do. One, empower the Federal Trade Commission. The FTC has a long bipartisan history of responding to constantly changing array of threats on behalf of the American people, but they're understaffed and they typically can't get penalties from wrongdoers when they break the law. That should change.

Second, Congress should pass legislation requiring companies to use reasonable data security. The FTC has interpreted its Section 5 authority to require reasonable security but they have been challenged in court and it's difficult, if not impossible, to attribute instances of harm to individual data breaches. We should have rules requiring reasonable security.

And, last, don't block the states from protecting their own citizens. Some level of preemption may be appropriate in a bill but states have to be allowed to pass protections for what a Federal bill doesn't cover. The states have been leaders on data security, passing the first breach notification laws, starting in 2002, and they have kept updating those laws over time so they don't just cover financial information, they cover other sensitive categories, like health data and e-mail and photo storage accounts. States need to be empowered to step in and protect their citizens when Federal protections are missing.

Thank you very much for inviting me to discuss these important issues. I look forward to answering any questions I can.

[The prepared statement of Mr. Brookman follows:]

PREPARED STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, PRIVACY AND TECHNOLOGY POLICY, CONSUMERS UNION

On behalf of Consumers Union, I want to thank you for the opportunity to testify today. We appreciate the leadership of Chairman Moran and Ranking Member Blumenthal in holding today's hearing to explore the still-developing field of bug bounty programs, and how they can best be implemented to promote data security for American consumers.

I appear here today on behalf of Consumers Union, the advocacy division of Consumer Reports, an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world.[1]

Consumers Union is a strong proponent of bug bounty programs, and believes that they play a crucial role in a data security ecosystem that has failed consumers far too often. Used properly, bug bounty programs enable companies to learn of breaches and vulnerabilities, in service to the larger goals of protecting consumer data and alerting consumers to threats as warranted and/or required by law. In the case of the 2016 Uber security incident, we believe the company should have disclosed the event earlier, not only because a hacker had accessed sensitive data, but because it appears credentials to that data had been publicly accessible for some time. This incident illustrates the continuing need for Congress to pass legislation providing stronger incentives for companies to deploy reasonable safeguards for personal data.

I. The Poor State of Modern Data Security and the Importance of Bug Bounty Programs

As this Committee well knows, the story of data security in recent years is not a pretty one. Massive data breaches have become commonplace, as companies accumulate vast troves of valuable consumer data but frequently fail to put adequate systems in place to protect it. The Target data breach of 2013 compromised the information of an estimated 110 million people,

including the payment card information of about 40 million consumers.[2] Hackers obtained the data of about 80 million people in the Anthem data breach of 2015.[3] And last year, criminals took advantage of well-known vulnerabilities in software used by Equifax to access the Social Security numbers of over 145 million people.[4] Targeted companies often have the opportunity to head off a breach but neglect to take action. For example, the software vulnerabilities that made Equifax a ripe target for attackers had been public for months, but Equifax failed to address them before the breach.[5]

Bug bounty programs represent a novel and innovative approach to identifying vulnerabilities before they can be taken advantage of by malicious actors. These programs incentivize a diverse third-party ecosystem to probe systems for potential failures. They also provide an alternative to sale of exploits on the black market where they can fetch several hundred thousand dollars—or more.[6] By offering to pay for information directly, companies can offer white- and grey-hat hackers a legal way to monetize their skills, with a far better outcome for companies and consumers. The rapid rise of these programs is evidence of their success. In 2016, Google paid out over $3 million under its bug bounty program for vulnerabilities in products such as Android and Chrome.[7] Last year it partnered with HackerOne to expand the program to cover popular third-party apps in its Google Play Store.[8]

Consumers Union strongly supports the development of bug bounty programs, not just by large tech companies, but for any company that stores sensitive consumer data that could lead to identity theft, harm, or embarrassment if exposed. In fact, bug bounty programs are identified as an indicator of good data security in the Digital Standard—an open source effort led by Consumer Reports to articulate best

---

[1] As the world's largest independent product-testing organization, Consumer Reports uses its more than 50 labs, auto test center, and survey research center to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

[2] Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement,* N.Y. TIMES, (May 23, 2017), *https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.*

[3] Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits over Data Breach,* REUTERS (Jun. 23, 2017), *https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML.*

[4] *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident,* EQUIFAX.COM (Oct. 2, 2017), *https://www.equifaxsecurity2017.com/2017/10/02/equifax-announces-cybersecurity-firm-concluded-forensic-investigation-cybersecurity-incident/.*

[5] Lily Hay Newman, *Equifax Officially Has No Excuse,* WIRED (Sep. 14, 2017), *https://www.wired.com/story/equifax-breach-no-excuse/.*

[6] Kif Leswig, *Here's what Apple thinks about the black market for $1 million iPhone hacks,* BUSINESS INSIDER, (Jul. 4, 2016), *http://www.businessinsider.com/apple-addresses-black-market-for-software-vulnerabilities-2016-6*

[7] Taylor Hatmaker, *Google's bug bounty program pays out $3 million, mostly for Android and Chrome exploits,* TECHCRUNCH, (Jan. 31, 2017), *https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/.*

[8] Liam Tung, *Android Security: Google will pay $1000 for holes in these top apps,* ZDNET, (Oct. 20, 2017), *http://www.zdnet.com/article/android-security-google-will-pay-1000-for-holes-in-these-top-apps/.*

practices for privacy, security, ownership, and governance in an increasingly connected world.[9] We launched the Digital Standard with our partners Ranking Digital Rights, Disconnect, and the Cyber Independent Testing Lab in March of last year as part of a strategic shift to start evaluating products for these values as part of our core reviews and ratings service.[10] In addition to highlighting the value of bug bounty programs, the Digital Standard defines as best practices "disclos[ing] the time-frame in which it will review reports of vulnerabilities" and—notable for this hearing—"commit[ting] not to pursue legal action against security researchers."[11]

II. "John Doughs" and the Uber Bug Bounty Program

Although open source software development has always depended on external support to identify errors and weaknesses in code, formal bug bounty programs within major technology companies are still a relatively new phenomenon. As such, it is understandable that expectations, norms, and best practices are still developing in this area.

In 2016, a hacker calling himself "John Doughs" e-mailed Uber's chief security officer Joe Sullivan that he had discovered a "major vulnerability" in Uber's systems.[12] In subsequent conversations with the hacker, Uber discovered that company engineers had posted credentials to Uber's servers on the code management portal GitHub, and that Doughs had used the credentials to access information about Uber's 57 million user and driver accounts, including sensitive data such as driver's license numbers. Although Uber told Doughs that its maximum bug bounty payout was $10,000, the hacker insisted that he expected "six digits" for his information. Eventually, Uber decided to pay Doughs $100,000, and required him to agree to delete the compromised data.

In general, we believe it is counterproductive to report participants in bug bounty programs to law enforcement absent a strong indication of malicious intent. We are not convinced there is anything wrong *per se* with a hacker asking for more money than is originally offered for information on a vulnerability. A hacker may reasonably believe that the value of the information and the time invested in uncovering it merit a higher payment. In the past, others have criticized Uber's bug bounty program for failing to provide reasonable payments for identifying exploitable holes in their code.[13] At some point, a request for more money may convey an implicit—or explicit—threat to sell the exploit or compromised data elsewhere if the demands are not met. However, from the publicly reported facts, it is not clear that that happened in this case. In any event, Uber had invited persons such as Doughs to look for precisely the type of vulnerabilities that he eventually found. If security researchers have to worry that looking for bugs in code will lead to criminal referral, the efficacy of bug bounty programs will dramatically decrease.

Nevertheless, Uber had an ethical—and legal—obligation to be more forthcoming with its users after it was made aware of its security lapse. Forty-eight states—as well as the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have laws mandating disclosure to consumers when their personal information is jeopardized in a security breach.[14] Drivers' license information—which was compromised in this incident—is typically included within such laws. While breach notification triggers vary significantly among the states, it seems quite likely that at least some state laws mandated disclosure to Uber drivers about the incident. For example, California law requires breach notification when "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." While many other states only require notification upon a determination that no harm was likely to have occurred, it is not clear how Uber could have reasonably come to this conclusion. Even if Uber felt it could trust that John Doughs had not sold or copied the data, Uber knew that credentials to its servers had been publicly accessible in Github and could have been used by others to access sensitive

---

[9] The Digital Standard, *https://www.thedigitalstandard.org/*.

[10] Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security, CONSUMER REPORTS, (Mar. 6, 2017), *https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/*

[11] The Digital Standard, Data Security, Vulnerability disclosure program, *https://www.thedigitalstandard.org/the-standard.*

[12] Nicole Perlroth and Mike Isaac, *Inside Uber's $100,000 Payment to a Hacker, and the Fallout,* N.Y. TIMES, (Jan. 12, 2018), *https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html.*

[13] Gregory Perry, *How I Got Paid $0 From the Uber Security Bug Bounty,* MEDIUM, (Dec. 24, 2017), *https://medium.com/bread-and-circuses/how-i-got-paid-0-from-the-uber-security-bug-bounty-aa9646aa103f*

[14] Security Breach Notification Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES, (Apr. 12, 2017), *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.*

personal information.[15] Uber is in constant communication with its drivers and could easily have told them about the potential exposure of their information; instead they decided to say nothing.

State data breach notification laws were first passed starting in 2002, and were clearly not written with bug bounty programs in mind. Notification laws and bug bounty programs both play an important role in protecting consumers, but there is a potential conflict between the two that needs to be reconciled. Indeed, notifying consumers of breaches created by ethical hacking pursuant to bug bounty programs could unnecessarily alarm consumers without providing any clear benefit.[16] Lawmakers seeking to update these protections must be extremely careful to balance the security benefits provided by external hacking with the right of consumers to know when their information is truly at risk, perhaps by developing general standards to govern the legitimate use of these programs. In any event, Uber was not entitled to simply decide not to follow consumer protection (and other) laws it believed to be onerous or unnecessary. Uber previously took over six months to announce a different data breach in 2015, making the delay in announcing the 2016 breach all the more difficult to justify.[17] Further, if in fact a condition of the payment to Doughs was that he could not disclose the incident—even after the vulnerability had been remedied so no one could exploit it—then the lack of transparency from Uber is still more concerning.[18]

III. New Laws are Needed to Provide for Better Security Incentives

Bug bounty programs should continue to play an important role in safeguarding consumers personal information. And Consumer Reports is committed to providing more information to the marketplace about which companies perform best under the Digital Standard, including which companies have the best security practices.

However, due to a misalignment of incentives, most companies today do not adequately invest in cybersecurity. Many breaches are not detected or publicly disclosed. The likelihood of law enforcement under the current regulatory scheme is low. The potential profits from using consumer data far outweigh any penalties that can be assessed for violations, incentivizing carelessness and misuse. And companies that experience a data breach bear only a portion of the cost—much of that instead is laid on consumers. As such, we need a much stronger data security law in the United States.

Americans lost an estimated $16 billion to identity theft in 2016, up almost $1 billion from the year prior.[19] Department of Justice data reveals that about 7 percent of Americans over the age of 16 experienced identity theft in 2014.[20] About 9 percent spent a month or more repairing their accounts or credit histories.[21] Tax identity theft—when identity thieves use compromised social security numbers to file taxes and collect the refund—is a significant concern as well. In Fiscal Year

---

[15] Jeremy Kahn, *Uber Hack Shows Vulnerability of Software Code-Sharing Services,* BLOOMBERG, (Nov. 22, 2017), *https://www.bloomberg.com/news/articles/2017–11–22/uber-hack-shows-vulnerability-of-software-code-sharing-services.* This was not the first time Uber credentials posted to GitHub led to a data security incident; in 2014, credentials posted in a publicly available GitHub repository compromised the data of 50,000 users. *Id.*

[16] Similarly, security researchers have called for modifications to the Wassenaar anti-proliferation agreement to allow for cross-border communications about security vulnerabilities and the effective management of bug bounty programs. *See* James Sanders, *How the Wassenaar Arrangement threatens responsible vulnerability disclosures,* TECHREPUBLIC, (Jul. 7, 2015), *https://www.techrepublic.com/article/how-the-wassenaar-arrangement-threatens-responsible-security-vulnerability-disclosures/.*

[17] Dave Lewis, *Uber Suffers Data Breach Affecting 50,000,* FORBES, (Feb. 28, 2015), *https://www.forbes.com/sites/davelewis/2015/02/28/uber-suffers-data-breach-affecting-50000/#5e59102c2db1.*

[18] Mike Isaac, Katie Brenner, and Sheera Frankel, *Uber Hid 2016 Data Breach, Paying Hackers to Delete Stolen Data,* N.Y. TIMES, (Nov. 21, 2017), *https://www.nytimes.com/2017/11/21/technology/uber-hack.html.* Even today, Uber and HackerOne, despite publishing statistics about the bug bounty program, appear to be omitting inclusion of this incident. The bounty program's webpage states that its top bounties range between $4,400 and $20,000, despite reports that John Doughs was paid over $100,000 for information about this security vulnerability. *See Uber: Bug Bounty Program,* UBER, *https://hackerone.com/uber.* This is despite the site denoting "AWS credential exposure resulting in access to driver documents" as an example of in-scope vulnerability class examples—precisely the vulnerability exposed by Doughs.

[19] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study,* JAVELIN (Feb. 1, 2017), *https://www.javelinstrategy.com/press-release/identity-fraudhits-record-high-154-million-us-victims-2016–16-percent-according-new.*

[20] U.S. Dep't of Justice, Victims of Identity Theft, 2014 1 (Sep. 2015), *https://www.bjs.gov/content/pub/pdf/vit14.pdf.*

[21] *Id.* at 10.

2016, the Internal Revenue Service discovered fraudulent returns filed for nearly 1 million people, totaling $6.5 billion.[22] And because consumers often cannot reliably attribute these losses to particular companies, those companies typically can't be held responsible in court for consumers' losses.

Congress needs to act to update consumer protections to reflect the extremely real threats poses to consumers by poor security practices.

First, lawmakers should give the Federal Trade Commission (FTC)[23] stronger resources and tools to protect consumers. The FTC has a long, bipartisan history of responding to an ever-changing array of threats on behalf of the American people. However, the agency does not have sufficient resources to police the marketplace as it should, and there are gaps in its authority to address privacy and data security lapses in various sectors. For example, it currently lacks the authority to take action against nonprofit entities and "common carriers."[24] Moreover, when it does bring a case against a bad actor, it typically lacks the authority to obtain civil penalties to deter potential wrongdoers from similar behavior. As such, deceptive or unfair business practices can be rationalized by companies as a (fairly low) cost of doing business.

Second, Congress should pass legislation requiring companies that have access to sensitive personal information to use reasonable security to safeguard it. Despite the FTC's long-standing use of the FTC Act to address data security lapses, some companies continue to challenge it.[25] The FTC to date has brought over 60 cases challenging shoddy data security practices, but given the uncertainties in application, challenges in attributing harm to specific incidents, and the lack of penalties, the market has yet to internalize the risks posed to consumers by potential data breaches.

Finally, while the vast majority of American citizens are protected by state data breach notification laws today, a Federal standard has the potential to strengthen these requirements and impose stronger penalties. However, the goal of any Federal breach notification law must be to strengthen consumer protections, not weaken the already inadequate incentives in place today. As a result, any such bill should include the resources and stronger authority for the FTC discussed above. Further, it must not broadly preempt state breach and security laws that cover information outside the scope of a Federal law.

Indeed, states must be allowed and encouraged to continue to innovate to protect their citizens. States have been the leaders in passing and revising data breach notification legislation over the years. At first, these laws primarily covered financial information such as Social Security numbers and credit card account numbers. However, over time, several states have extended these laws to cover new categories of information that, if compromised, pose risks to consumers. For instance, some states have extended breach notification protections to e-mail and photo storage accounts, recognizing that those databases contain incredibly personal information, and could be leveraged for new types of damaging identity theft.[26] States must be allowed to iterate over time to protect their citizens from new and emerging security threats.

Conclusion

Thank you again for the opportunity to testify here today about the challenges of implementing bug bounty programs to best safeguard personal information. We believe that these programs play a vital role in uncovering vulnerabilities in code before they can be exploited by malicious actors. However, in order to incentivize companies to deploy these and other data protection safeguards, Congress must update consumer protection laws for the modern age to account for the unprecedented threats to our personal data. I look forward to answering the Committee's questions.

---

[22] Written Testimony of John A. Koskinen Before the Senate Finance Committee on the 2017 Filing Season and IRS Operations, INTERNAL REVENUE SERV. (Apr. 6, 2017), *https://www.irs.gov/newsroom/writtentestimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operationsapril-6-2017.*

[23] From August 2015 to August 2017, I served as Policy Director of the FTC's Office of Technology, Research, and Investigation.

[24] Oral Statement of Commissioner Terrell McSweeny before the House Judiciary Committee, (Nov. 21, 2017), *https://www.ftc.gov/system/files/documents/public_statements/1268963/mcsweeny_oral_testimony_to_us_house_of_representatives_committee_on_the_judiciary_11-1-17_.pdf.*

[25] *E.g.,* Mallory Locklear, *FTC lawsuit over D-Link's lax router security just took a big hit,* ENGADGET, (Sep. 21, 2017), *https://www.engadget.com/2017/09/21/ftc-lawsuit-d-link-lax-router-security-took-hit/.*

[26] *E.g., Delaware Amends Its Data Breach Notification Law,* MAYER BROWN, (Aug. 29, 2017), *https://www.mayerbrown.com/delaware-amends-its-data-breach-notification-law-08-29-2017/.*

Senator MORAN. Thank you very much. Thank you all.

Let me start with some questions and I don't know whether we'll have time for a second round or not. So if we can have relatively brief answers, I'll try to have relatively brief questions.

First of all, for you, Mr. Flynn, what's the justification that there apparently was no, in the view of Uber, legal or other obligation to notify the victims of the hack?

Mr. FLYNN. Senator, there's no justification for that. We should have notified our customers at the time when this did occur and it was a mistake not to do so.

Senator MORAN. So Uber does not take the position that the law is unclear?

Mr. FLYNN. I do believe that the patchwork laws that are per state are a challenge for all companies and defenders to contend with. I do believe that is the case, but in this case, I think the real issue was that we didn't have all the right people in the room making that evaluation and making the right decision and making right by our customers.

Senator MORAN. Thank you for that honest answer.

Perhaps this is Mr. Mickos or Ms. Moussouris. Excuse me.

Ms. MOUSSOURIS. Like a dinosaur, Moussouris.

Senator MORAN. Moussouris. Thank you. That's very helpful. I'll be sitting here thinking if I get it right what dinosaur was that.

So what determines the price for which a hacker is paid for the return of the information? Is that a negotiated item and what are the factors that are determined, in this case a $100,000 being apparently appropriate?

Mr. MICKOS. Mr. Chairman, by now the world has paid tens of thousands of bounties. So there starts to be a typical pricing for any sort of vulnerability. So you can compare to other companies and you can set your bounties in accordance with common practices.

But the bounty decision is always a decision for the company who's receiving the vulnerability and the main influencing factor is the severity of the vulnerability, *i.e.,* how bad would it be if indeed a criminal abused the vulnerability, and that is why in my opening statement I said the average over all these bounties is only about $500 per vulnerability, but the highest bounties offered are $250,000. So it's mathematically a question of a power law distributed set where there are very few extremely valuable vulnerabilities that will catch a very high price all the way up today to $250,000 whereas the majority of the regular day-to-day bug bounty program operates in the range of hundreds or thousands of dollars.

Senator MORAN. What's the obligation to report the payment or the breach to law enforcement and once a bounty is paid, is that obligation changed? Is that part of the agreement?

Mr. MICKOS. Mr. Chairman, the business, the bug bounty program is a preventative service and it is not the function of incident response.

Senator MORAN. So in the case of your client, Uber, did you work for them? You were performing services for them prior to the incident of 2016?

Mr. MICKOS. Uber became a customer of HackerOne in 2015 and they operate their Bug Bounty Program on our platform, yes.

Senator MORAN. And so you did not determine a vulnerability prior to the realization that there was a problem in 2016?

Mr. MICKOS. The way we deal with it, the vulnerability gets reported through our platform. We do not see the contents of the report. It goes to the customer and the customer takes action and may come back to HackerOne and say this was a valid vulnerability report, please pay the following bounty to this hacker, and that is how we deal with any of these bounties when they come from any of our customers.

Senator MORAN. What are the other techniques, besides bug bounties? I said it in my opening statement, but I think you indicated, Ms.——

Ms. MOUSSOURIS. Moussouris.

Senator MORAN.—Moussouris—thank you so much for the reminder. Defensive hack ecosystem. So we've been focused on bug bounties, but there apparently are other techniques that we ought to be aware of?

Ms. MOUSSOURIS. Yes, of course. If I could answer your previous question about bounty price?

Senator MORAN. Please.

Ms. MOUSSOURIS. That is actually something that is very important in terms of the defense market.

There is a defense market for bugs and exploits and there is an offense market for bugs and exploits and they're characterized not just in price. There's a huge price differential, but they're characterized differently when it comes to what their objective is.

So the offense market for bugs is buying bugs and exploits that are fairly reliable and much higher priced in order to keep them secret and usable for attack purposes. They could be bought for regular law enforcement or used by nation states. They could be bought by criminal organizations.

Defensive bounty prices, which regular bug bounties are a part of the defensive market, there is a logical ceiling above which those defensive market prices cannot exceed. You cannot compete directly with the offense market.

The reason for that is you will create a perverse set of incentives where you might, you know, essentially incent some developers inside of an organization to collude with a member of the outside to write bugs into the code. You may create an environment where it's much more lucrative to spend your time hunting for bugs than it is to develop fixes or even develop new code.

So we're already seeing a skew in the market right now where the way that the bug bounties are being used and applied, where it is actually much more lucrative. I think HackerOne just released a report talking about how much more lucrative it is to be a bug bounty hunter than it is to be a developer and that's including in the United States.

So we do have to be mindful of this market that we're creating here and make sure that we're not over-skewing and over-rewarding the pointing out of flaws without creation of an ability to catch these bugs and deal with them appropriately and building that workforce.

So back to your——

Senator MORAN. Excuse me one moment.

Ms. MOUSSOURIS. Yes.

Senator MORAN. So I want to make sure I understand something because this is at least useful to me. It's not a question of whether you pay the consequences of the breach versus the amount of money that the bounty would be.

It seems to me that when Mr. Mickos says the maximum is $250,000, that's the compensation for finding the problem. It's not a competition between how much money I'm going to pay to find the problem after there has already been a problem because the consequences of the hack will be much more expensive than the $250,000 maximum that Mr. Mickos—do I understand something here?

Ms. MOUSSOURIS. Well, it is hard to estimate the overall cost of a breach. It's hard to estimate it to the company involved, to the users whose data may be compromised, and to other, you know, affected and related systems.

So there should not actually be a direct correlation between the resulting potential harm and a defensive market price. It is much more of a token of appreciation, even if it is a six-figure payout, and I created Microsoft's Vulnerability, you know, Bug Bounty Program at $100,000 but it was for a technique. That is something that's sufficiently rare that it wasn't creating these perverse incentives where, you know, people could quit working at Microsoft, stop working on platform mitigations, and instead go off and, you know, supply these.

Whereas the damage that, you know, potential new exploitation technique could cause in the ecosystem is certainly much more multiple millions of dollars. It is the idea of setting these incentives at an appropriate level where you are drawing out interest and creativity of the hacker community to work with you, but not setting them so high for something that is not sufficiently rare enough that you're not creating this much more lucrative business.

And in the case of these breaches, what I'm concerned about as, you know, a concerned member of the defensive economy here is that why would a hacker turn in a bug and follow the rules for $10,000 when the term "bug bounty" has been muddied to include downloading 57 million records and getting paid a $100,000 for that data theft?

I think that is a line that we should be very, very clear that bounties should not be negotiable in that way. You had asked that question. Should they be negotiable? I think not. They are about setting what you think is a reasonable price, such that you're below that, you know, perverse incentive mark of inciting some bad actors and some bad activities and really setting an example for the hackers of today and the hackers of tomorrow to participate in the defensive economy for bugs in the right way.

Senator MORAN. Thank you very much.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Senator Moran.

I think this distinction is pretty simple and I think you make it in your testimony, Ms. Moussouris, when you say that we need to make clear that only "the minimum necessary proof is required to

prove that a vulnerability exists and that no further access or exploitation passed that point is authorized."

And actually, Mr. Flynn, you make it pretty clear, too, when you say in your testimony, "in my view, the key distinction regarding this incident is that the intruders not only found a weakness, they also exploited the vulnerability in a malicious fashion to access and download the data."

It's the difference between a security consultant who says about your home, you have this vulnerability to forced entry and the criminal who says you have this vulnerability to forced entry and I have your child, pay me a $100,000. That's ransom. It's a crime.

And so concealing it, in my view, is in effect aiding and abetting that crime. I don't know what you want to call it, but wouldn't you agree with me that the net effect was to cover up or seek to cover up a crime?

Mr. FLYNN. Mr. Blumenthal, thank you for those points.

I agree that this was not consistent with the way in which our Bug Bounty Program normally operates and it's important to understand that this is not the way that we're going to do these things moving forward.

You know, I think that, as you point out, sir, the fact that this was a multistep malicious intrusion, a downloading of data, and an extortion and ransom demands, means that this wasn't consistent with that or the way that that program normally operates.

Senator BLUMENTHAL. And any such criminal conduct needs to be reported immediately to authorities.

Mr. FLYNN. Yes, sir, exactly.

Senator BLUMENTHAL. And to consumers, ordinary people, whose lives may be put at risk as a result.

Mr. FLYNN. I agree with you on both counts, sir. I think we made a misstep in not reporting to consumers and I think we made a misstep in not reporting to law enforcement and those are both things that we have corrected and will correct going forward.

Senator BLUMENTHAL. Would you agree with me, actually with the Electronic Privacy Information Center that "bug bounties need to be non-negotiable and clearly defined in company policy. Otherwise, companies are letting user data be held as ransom."

Mr. FLYNN. I do believe it's important to understand the boundaries between our Bug Bounty Program and a case like this which had those features that you had pointed out, the extortion and ransom demands and so forth.

Senator BLUMENTHAL. Extortion and ransom demands but also when you say you're going to run a bug bounty program, if you say we're going to negotiate with you when you have access to our information or when you have the information, it exposes you in effect to extortion and ransom demands, correct?

Mr. FLYNN. Yes, sir, and what I would recommend, after learning a lot of lessons from this experience personally, is that I would recommend all companies that are running and operating bug bounty programs to ensure that they have a process and procedure in place for when and if this type of occasion does occur because I think it's something that we hadn't contemplated at the time and we made some missteps along the way as a consequence.

Senator BLUMENTHAL. Does Uber have that procedure in place now?

Mr. FLYNN. So we have changed a number of aspects of our approach. One of the things that we didn't do well here is that we didn't include enough of the right legal representatives to determine if this was a data breach notification requirement. So we've done one thing, which is brought everybody into the room. I think we've done another thing where we've made sure that we——

Senator BLUMENTHAL. Let me just because my time is running out——

Mr. FLYNN. Oh, sorry.

Senator BLUMENTHAL.—ask you, do you have clear limits, parameters, for non-negotiable and clearly defined policy on how much you will pay?

Mr. FLYNN. Yes, as part of new leadership coming in, we are in the process of reviewing and updating our policy regarding that right now.

Senator BLUMENTHAL. So you don't have them now but you're——

Mr. FLYNN. It's something we are working on and we've also brought in Matt Olsen, the former General Counsel of the National Security Agency, to help guide us, as well.

Senator BLUMENTHAL. Mr. Mickos, does HackerOne have those kinds of policies in place?

Mr. MICKOS. We do.

Senator BLUMENTHAL. Clear brackets or parameters?

Mr. MICKOS. Senator, we do have policies. We do not engage in extortion payouts. That's against our policies. It's not the business we are in.

Senator BLUMENTHAL. My time has expired. In deference to the other members of the Committee, I'm going to stay within the limit. I'm hoping that maybe we'll have another round.

I would—while I'm remembering to do it, I have three documents I'd like to submit for the record. A written statement by Kathleen McGee, Chief of the Bureau of Internet and Technology for the New York State Office of Attorney General. Her statement highlights the important role of State Attorneys General in protecting consumers and enforcing data security protections.

The second is the letter, dated February 5, 2018, from Representatives Schakowsky and Lujan, and the third is the letter, also dated February 5, from the Electronic Privacy Information Center.

Senator MORAN. Without objection, they'll be entered.

[The information referred to follows:]

PREPARED STATEMENT OF KATHLEEN MCGEE, CHIEF OF THE BUREAU OF INTERNET & TECHNOLOGY, NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL

Chairman Moran, Ranking Member Blumenthal, and other distinguished Members of the Subcommittee:

My name is Kathleen McGee, and I am the Chief of the Bureau of Internet & Technology at the New York State Office of the Attorney General, Eric T. Schneiderman. The Bureau of Internet & Technology is responsible for protecting New Yorkers from existing as well as new and developing online threats.

I am pleased to present this prepared testimony concerning data breaches, which continue to victimize consumers with greater and greater frequency, from small local businesses to giants like Target, Anthem, Yahoo, Equifax, and Uber.

In late November 2014, the New York Attorney General's Office opened an investigation into Uber's collection, maintenance and disclosure of riders' personal information amidst reports that Uber executives had access to riders' locations and that Uber displayed this information in an aerial view, known internally as "God View." Separately, Uber notified our office that, as early as September 2014, it had experienced a data breach where Uber driver names and driver's license numbers were accessed by an unauthorized third party.

In a settlement resolving those allegations, Uber agreed, among other things, to:

- Maintain and store GPS-based location information in a password-protected environment, and encrypt the information when in transit.
- Limit access to geo-location information to designated employees with a legitimate business purpose, and enforce this limitation through technical access controls, and a formal authorization and approval process;
- Designate one or more employees to coordinate and supervise its privacy and security program;
- Conduct annual employee training to inform employees who are responsible for handling private information about Uber's data security practices;
- Adopt protective technologies for the storage, access, and transfer of private information, and credentials related to its access, including the adoption of multifactor authentication, or similarly protective access control methodologies;
- Conduct regular assessments of the effectiveness of Uber's internal controls and procedures related to the securing of private information and geo-location information and the implementation of updates to such controls based on those assessments; and
- Maintain a separate section in its consumer-facing privacy policy describing its policies regarding location information collected from riders.

Despite those commitments, reports surfaced late last year that Uber experienced yet another data breach affecting 57 million riders and drivers. Worse yet, Uber reportedly kept the data breach secret for more than a year after paying a $100,000 ransom.

These deeply concerning reports led the New York Attorney General's Office to open an investigation into this breach and Uber's associated conduct. While I cannot share details from ongoing investigations, I can say we are getting to the bottom of this Uber breach, and that we take very seriously drivers' and riders' right to the protection of sensitive information they entrust to Uber.

States have a central role in protecting consumers and their data. The New York Attorney General's Office and other State Attorneys General offices have been policing data breaches for nearly two decades. In fact, State Attorneys General frequently work cooperatively, in collaboration with each other and relevant Federal agencies, to protect consumers in this area.

Indeed, the states have led the way on data protection for consumers. When the Internet was still relatively new to consumers, states responded with data protection and data breach laws to protect their residents. And as the technology has evolved over the years, state law has evolved with it.

Back in 2002, when the Internet was younger and e-commerce was beginning to take off, California enacted the first data breach notification law. It proved to be a tremendous success for consumer protection, and New York and other states soon followed. Today, 48 states, the District of Columbia, and U.S. territories all have data breach notification laws. That is the sort of innovation at the state level that our Federal system, at its best, promotes.

The states have already adapted those laws as technology and consumers' use of it changed, and as new threats emerged. For example, as e-mail and other online accounts became an increasing part of consumers' daily lives—to make appointments, send confidential documents, and discuss work and personal affairs—account credentials became the "keys to the castle" for consumers' data.

As a result, states amended their laws to add username-and-password combinations as a trigger for breach notification—a key state law innovation. This is just one of many examples. As companies increasingly used fingerprints to unlock devices, state laws began covering biometric data.

But it is better to prevent breaches before they happen. And states have been equally innovative on this point: enacting legislation requiring companies to implement adequate data security, and updating such laws as technology evolves. And states have a second tool: consumer protection laws, which State Attorneys General use to police misrepresentations about data security—as with other consumer prod-

ucts, it can be unlawful for a company to make misrepresentations about data security to consumers.

The New York Attorney General's office, recognizing the importance of this issue for consumers and the need to update New York's law, has proposed legislation to update New York's data security and breach notification laws. And, the New York Department of Financial Services—a separate state agency with jurisdiction over New York's banking and insurance sectors—also has innovated in this area, implementing important data security regulations to protect consumers' financial data.

In light of this background, I would like to make a few key points.

First, it would be a big mistake for Congress to preempt states' ability to legislate and innovate in this area. The law must be able to keep pace with the ever-increasing rate of change in technology. States have proven the ability to act quickly in that regard—from both legislative and enforcement perspectives. In contrast, bills have been proposed in Congress for many years but, for one reason or another, enactment has proven elusive. Even if a Federal law were enacted, it could prove difficult to amend and would fall far behind new technologies that will inevitably continue to emerge. Thus, even a Federal law providing the most stringent protections based on current state requirements will leave consumers more and more vulnerable over time.

Second, when it comes to enforcement, states occupy a leading role today and must continue to do so.

Our office has issued data breach reports in recent years that show an alarming increase in data breaches. Indeed, in 2016 we received 1,300 data breach notices—up 60 percent from the year before. This Committee is likely aware of the megabreaches, such as the Target breach involving 40 million credit card numbers and the Anthem breach involving over 78 million records including Social Security Numbers. In those instances, New York and other states used a well-established process to coordinate enforcement efforts against companies that violated consumer trust with inadequate data security. As a result, the states obtained not just data security reforms through injunctive relief but also large civil penalty recoveries that are essential to deterring other companies from violating consumer trust through lax security practices.

Less well-known, yet equally important, are the enforcement actions our office takes in response to smaller breaches that occur by the hundreds each year in New York and other states. One recent case illustrates the point. A small company outside Buffalo, New York misconfigured a web server, which led to the disclosure of 500 employment applications with Social Security Numbers in Google search results. Our office found out through a tip, contacted the company immediately, and got the applications removed from search results within days.

Even if a Federal agency were provided with the most comprehensive data security law and the considerable resources needed for serious enforcement, it is unlikely that a Federal agency would be as responsive as our office and our sister State Attorneys General to breaches involving local businesses and relatively small numbers of local consumers. These breaches may be smaller than a Target or an Equifax or an Uber—but the victims are no less in need of law enforcement protection. Smaller breaches like these are the rule, not the exception.

Further, with years of first-hand experience policing data security in our state, we know how to distinguish between breaches that a company should have prevented with better security versus breaches that could not have been avoided despite the company's reasonable security practices. By virtue of this experience, and our knowledge of conditions within our local communities and industries, we can avoid both underenforcement that would leave consumers unduly vulnerable and overenforcement that would create undue burdens on local businesses.

For all of these reasons, I respectfully urge this body to ensure that any legislation it considers meets the following requirements, which are vital to protecting states' innovative role in consumer data protection:

- Any new Federal requirements should not preempt state law, but instead should expressly set a floor—not a ceiling—on data security standards and protocols in the event of breaches. States must be able to innovate in the areas of data security and breach notification and pass stronger and more up-to-date laws than the Federal standard.
- As with several other Federal consumer protection laws, any Federal requirements must be enforceable by State Attorneys General in addition to a Federal agency, and any Federal penalties or other monetary relief must be recoverable by the states as well.
- To the extent any preemption language is included, beyond the floor/ceiling issue discussed above, the language must be drawn carefully to avoid unin-

tended severe consequences. Some preemption language can be so broad that it might be interpreted to set aside state laws concerning personal privacy or computer crimes, and that would be a serious problem for constituents.

These or similar provisions for joint Federal and state enforcement authority are already included in other Federal laws and have proven successful. For example, the New York Attorney General's office has coordinated with the FTC on several investigations into violations of the Federal Children's Online Privacy Protection Act, or COPPA, to stop invasive tracking on major child-focused websites.

The vast majority of State Attorneys General have similarly called on Congress to avoid preempting state action on data security, as recently as 2015, when a broad bipartisan group of 45 State Attorneys General joined in asking Congress to oppose then-pending data security bills with harmful preemption provisions.

Our office continues to enforce data security protections on behalf of New Yorkers and to work with New York's state lawmakers to continually update those protections. We appreciate your Committee's efforts to complement those efforts at the Federal level while ensuring that work at the state will continue successfully.

Congress of the United States

Washington, D.C. 20515

February 5, 2018

The Honorable Jerry Moran
Chairman
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security
Committee on Commerce, Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Richard Blumenthal
Ranking Member
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security
Committee on Commerce, Science, and Transportation
716 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Moran and Ranking Member Blumenthal:

We are writing in advance of your hearing titled "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers" to call your attention to Uber's concealment of its 2016 data breach from the Federal Trade Commission (FTC) as it negotiated a consent agreement with the FTC for an earlier breach. We believe that Uber must be held accountable for withholding this information from the FTC. We recently sent a letter to the FTC urging the agency to reopen the consent agreement and reevaluate the adequacy of the remedies imposed on Uber for privacy violations.[1] We have attached a copy of our letter to the FTC for your reference.

Many facts about Uber's year-long cover-up of a breach that affected 57 million customers and drivers are still unknown.[2] We do know, however, that the breach occurred in October 2016, Uber's security team became aware of it in November 2016, and Uber did not notify the FTC until a year later, on November 21, 2017.[3] During that intervening year, as Uber employees were arranging a $100,000 ransom to recover the data and keep the 2016 breach quiet, the FTC was investigating a smaller 2014 data breach and actively negotiating a settlement with Uber regarding that 2014 breach. Uber signed a consent agreement with the FTC on August 15, 2017, without ever informing the agency of the second, much larger breach—one that

[1] Letter from Rep. Jan Schakowsky and Rep. Ben Ray Luján to Maureen Ohlhausen, Acting Chairman, Federal Trade Commission (Dec. 21, 2017).

[2] Letter from Dara Khosrowshahi, CEO, Uber Technologies, Inc., to Sen. John Thune, Chairman, Senate Committee on Commerce, Science, and Transportation, et al. (Dec. 11, 2017).

[3] *Id.*

PRINTED ON RECYCLED PAPER

resulted from a failure to correct the very security vulnerabilities that the FTC investigation of the 2014 breach exposed.[4]

It remains unclear who within the company was aware of the breach for the year preceding disclosure to the FTC. Uber has indicated that two employees were fired for "failing to disclose the incident to the appropriate parties," implying that the breach was not widely known within the company.[5] But it now appears that Uber's former CEO, the legal and communications departments, and as many as 50 engineers may have been involved.[6] Uber's response to the breach was even praised in end-of-year performance reviews of security personnel.[7] It defies credulity that there was not at least some overlap between those aware of the 2016 breach and those responding to the FTC investigation of the 2014 breach. Uber's concealment of critical facts as it negotiated with the FTC is extremely concerning.

Thank you to your Committee for bringing attention to this important issue. We urge you to explore what appears to be serious misconduct by Uber to hide information that would likely have resulted in stronger sanctions in the FTC enforcement action.

Sincerely,

Jan Schakowsky
Ranking Member
House Subcommittee on Digital Commerce
and Consumer Protection

Ben Ray Luján
Member
House Subcommittee on Digital Commerce
and Consumer Protection

Attachment: December 21, 2017 letter to FTC Acting Chairman Maureen Ohlhausen

cc: The Honorable John Thune
The Honorable Bill Nelson

---

[4] Federal Trade Commission, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017).

[5] *See* note 2.

[6] *Inside Uber's $100,000 Payment to a Hacker, and the Fallout*, New York Times (Jan. 12, 2016).

[7] Nicole Perlroth (@nicoleperlroth), Twitter (Jan. 12, 2018, 3:38 PM) (twitter.com/nicoleperlroth/status/951961492806541314).

Congress of the United States
Washington, DC 20515

December 21, 2017

Maureen K. Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Acting Chairman Ohlhausen:

I am writing to express my concern regarding recent revelations that Uber Technologies, Inc. was actively concealing a massive data breach at the same time it was negotiating a settlement with the Federal Trade Commission (FTC) for poor privacy and data security practices. In light of this new information, I ask that you consider reopening the public comment period and reevaluate the adequacy of the remedies imposed on Uber in the proposed settlement.

On November 21, 2017, Uber disclosed for the first time that the personal information of 57 million Uber riders and drivers had been stolen by hackers in late 2016.[1] Instead of notifying law enforcement and the public of the breach, Uber paid the hackers a $100,000 ransom in exchange for an agreement to destroy the stolen information and keep the incident secret.[2] Uber took steps to conceal the incident by pushing the hackers to sign nondisclosure agreements and disguising the ransom as legitimate payments from a bug bounty program.[3]

At the same time that Uber was covering up the 2016 breach, the company was negotiating a consent agreement with FTC to address earlier privacy and data security violations.[4] FTC announced the proposed consent on August 15, 2017, before the 2016 breach was made public and presumably without considering the massive scale of the 2016 breach and Uber's cover-up in deciding what remedies were needed to adequately protect consumers.[5] The proposed consent relates to a smaller 2014 breach affecting the personal information of more than 100,000 Uber drivers.[6] FTC's administrative complaint charged Uber only with deceptive practices for making false and misleading statements about its privacy policies.[7] Unlike other recent FTC data security cases, the Uber complaint did not include any charges that the

---

[1] Uber Technologies, Inc., *2016 Data Security Incident* (Nov. 21, 2017) (press release).

[2] *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, New York Times (Nov. 21, 2017).

[3] *Id.*

[4] Federal Trade Commission, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017) (press release).

[5] *Id.*

[6] *Id.*

[7] *Id.*

PRINTED ON RECYCLED PAPER

company engaged in unfair practices for failing to adequately protect the information it collected.[8] The proposed administrative consent prohibits Uber from misrepresenting its privacy policies and requires Uber to implement specific steps to enhance its privacy protections and submit to third party auditing.[9] The consent did not include any monetary relief.[10]

Uber's conduct indicates a troubling pattern of disregard for accountability and transparency with respect to its handling of users' personal information. In a statement responding to the proposed agreement, Uber claimed it had "significantly strengthened [its] privacy and data security practices" since 2014.[11] But both the 2014 and 2016 breaches occurred because Uber left employee login credentials exposed in code posted on Github, an online code-sharing repository.[12]

Uber has also repeatedly deceived the public about its privacy practices. The proposed consent agreement addresses Uber's use of a tool known as "God View" to secretly track users without proper notice or oversight.[13] But it does not address the use of another tool known as "Greyball" used to secretly track and evade regulators, which was only disclosed by Uber after a *New York Times* investigation in March 2017.[14]

Dara Khosrowshahi, Uber's new C.E.O. as of August 2017, has since made some changes at Uber in an attempt to distance the company from its previous misconduct, branding it "Uber 2.0."[15] However, larger questions remain about Uber's commitment to meaningfully reforming its leadership and company culture. Only two Uber employees were fired in response to the 2016 breach and subsequent cover-up.[16] Furthermore, Travis Kalanick, Uber's cofounder and C.E.O. until June 2017, still controls a majority of Uber's voting shares and three seats on the company's board of directors.[17] Mr. Kalanick reportedly knew of the 2016 breach and Uber's payments through the bug bounty program since November 2016.[18]

---

[8] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (Aug. 24, 2015) (company's failure to maintain reasonable data security for sensitive personal information resulting in breach fell within the plain meaning of an "unfair" act or practice in violation of Section 5 of FTC act).

[9] *See* note 4.

[10] *See* note 4.

[11] *Uber Agrees to 20 Years of Privacy Audits to Settle FTC Data Mishandling Probe*, TechCrunch (Aug. 15, 2017).

[12] *Uber Hack Shows Vulnerability of Software Code-Sharing Services*, Bloomberg (Nov. 22, 2017); *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg (Nov. 21, 2017).

[13] *Uber Agrees to Privacy Audits in Settlement with F.T.C.*, New York Times (Aug. 15, 2017).

[14] *Uber Settles U.S. Allegations Over Data Privacy*, Reuters (Aug. 15, 2017); *How Uber Deceives the Authorities Worldwide*, New York Times (Mar. 3, 2017).

[15] *Uber 2.0: New C.E.O. Wants to Put His Stamp on the Company*, New York Times (Nov. 9, 2017).

[16] *See* note 2.

[17] *In Power Move at Uber, Travis Kalanick Appoints 2 to Board*, New York Times (Sep. 29, 2017); *Uber Founder Travis Kalanick Resigns as C.E.O.*, New York Times (Jun. 21, 2017),

[18] *Exclusive: Uber Paid 20-Year-Old Florida Man to Keep Data Breach Secret –Sources*, Reuters (Dec. 6, 2017).

Uber's decision to keep the 2016 breach secret for nearly a year raises serious concerns about whether Uber was negotiating with FTC in good faith, and about whether the company has the intention and ability to properly administer the proposed consent. I therefore request a briefing on this matter with my staff and Committee staff. Please be prepared to discuss the following questions.

1. When did Uber first inform FTC of the 2016 breach and Uber's response? Was FTC aware of the 2016 breach and Uber's response when the Commission approved the proposed consent in August 2017?

2. It is our understanding that at least 20 Uber employees, as well as the C.E.O., were aware of the 2016 breach at the time Uber was negotiating with FTC. Given this, was the termination of only two employees in response to the 2016 breach sufficient to ensure the culture has changed and that Uber is likely to comply with the proposed consent?

3. Did Uber fail to comply with the terms of any civil investigative demand by withholding documents, information, or other relevant evidence related to FTC's investigation, including any evidence related to the 2016 breach and the company's response?

4. Did Uber violate any laws or regulations, including provisions related to preservation of records or making false statements, by destroying any evidence, by failing to disclose the 2016 breach and its response to that breach in the course of FTC's investigation, or any other action?

5. Is FTC conducting a separate investigation of Uber's "Greyball" tool? Did the Commission consider Uber's use of the "Greyball" tool when voting to approve the proposed consent?

6. Given that the 2014 breach involved personal information from over 100,000 Uber drivers including, for a subset of those drivers, Social Security number and bank account numbers, why did FTC not challenge the breach as both deceptive and unfair?

7. Has the Commission considered whether consumers would be better served if the Commission reopened its case against Uber and issued a new complaint in federal court, under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), that would include new charges on the 2016 breach and cover-up and seek broader remedies, including monetary relief?

Your assistance in this matter is greatly appreciated.

Sincerely,

Ben Ray Luján
Member
Subcommittee on Digital Commerce
and Consumer Protection

Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, February 5, 2018

Senator JOHN THUNE, Chairman,
Senator BILL NELSON, Ranking Member,
U.S. Senate Committee on Commerce, Science, and Transportation,Russell Senate Office Building, Room 253
Washington, DC 20002

Dear Chairman Thune and Ranking Member Nelson:

We write to you regarding the upcoming hearing on "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers."[1] The Electronic Privacy Information Center ("EPIC") supports initiatives, including payments to outside computer security experts, that prompt companies to fix vulnerabilities as this makes user data

more secure. But Uber disguised a blackmail payment as a bug bounty payment and waited over a year to disclose the breach of personal data to authorities and to consumers. Bug bounty programs do not excuse non-compliance with data breach notification laws.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues in the information age. EPIC is a leading consumer privacy advocate and has played a key role in developing the authority of the Federal Trade Commission ("FTC") to safeguard the privacy rights of consumers.[2] EPIC's complaint[3] concerning Google Buzz provided the basis for the FTC investigation and subsequent settlement, and the Commission's settlement with Facebook also followed from a complaint filed by EPIC and a coalition of consumer privacy organizations.[4]

Uber's privacy and security practices have been of particular concern to EPIC. EPIC filed a complaint[5] with the FTC in 2015 regarding Uber's egregious misuse of personal data. That complaint led to an FTC settlement[6] with Uber in August 2017. In 2015, EPIC also proposed a privacy law for Uber and other ride-sharing companies.[7]

It is important for this Committee not to lump in Uber's actions with legitimate payments to computer security experts. Bug bounty programs are used in both the public and private sectors to identify vulnerabilities. Blurring the line between bug bounties and breaches hurts white hat hackers who want to disclose vulnerabilities in an ethical way. Joe Sullivan, Uber's chief security officer (who has since been fired), denied that the 2016 incident was a breach and said the company had treated it as an authorized vulnerability disclosure.[8] But e-mails between Uber and the hacker reveal more complicated circumstances. After Uber told the hacker that the max payout of their bug bounty program was $10,000, he responded that he expected at least $100,000 and then threatened the company.[9]

Bug bounties need to be non-negotiable and clearly defined in company policy, otherwise companies are letting user data be held as ransom. $100,000 could have been an appropriate bounty for Uber to pay. Last month Google paid a security re-

---

[1] *Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers,* 115th Cong. (Feb. 6, 2018), S. Comm. on Commerce, Science, & Transportation, *https://www.commerce.senate.gov/public/index.cfm/hearings?ID=73871FA8-29AD-4ED5-ABB8-C86B4BE4E0A3.*

[2] *See, e.g.,* Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), *http://epic.org/privacy/internet/ftc/ftc_letter.html.*

[3] *In re Google Buzz* (2011), *https://epic.org/privacy/ftc/googlebuzz/.*

[4] *In re Facebook, Inc.* (2011), *https://epic.org/privacy/inrefacebook/.*

[5] EPIC Complaint to the FTC, *In the Matter of Uber Technologies, Inc.* (June 22, 2015), *https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.*

[6] Agreement Containing Consent Order FILE NO. 1523054, *In the Matter of Uber Technologies, Inc., https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_agreement.pdf.*

[7] Marc Rotenberg and Julia Horwitz, *Privacy Rules for Uber,* HuffPost (Feb. 11, 2015), *https://www.huffingtonpost.com/julia-horwitz/privacy-rules-for-uber_b_6304824.html.*

[8] Nicole Perlroth and Mike Isaac, *Inside Uber's $100,000 Payment to a Hacker, and the Fallout,* N.Y. Times (Jan. 12, 2018), *https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html?_r=0.*

[9] *Id.* (One e-mail read: "Yes we expect at least 100,000$ I am sure you understand what this could've turned out to be if it was to get in the wrong hands, I mean you guys had private keys, private data stored, backups of everything, config files etc. . . . This would've heart [sic] the company a lot more than you think.")

searcher $112,500 for an Android bug[10] and Apple offers up to $200,000 for iOS and iCloud bugs.[11] But the communications between Uber and the hacker make the $100,000 payment look more like extortion than a payment for services.

More critically, bug bounty programs do not exempt companies from data breach notification laws. Even though Uber obtained assurances that the downloaded data had been destroyed,[12] it was still required under state laws to notify users and authorities of the data breach. Once Uber was aware that user data had been compromised, it had a legal obligation to notify those affected by the breach. Waiting over a year to disclose is a clear violation of state data breach notification laws, most of which require a company to notify affected users within 30 or 45 days.[13]

The legal avenues for security researchers and white hat hackers to disclose vulnerabilities need to be more clearly defined. Most companies—94 percent of the Forbes Global 2000 to be exact—do not have a published vulnerability disclosure policy and because of this nearly one in four hackers have not reported a vulnerability that they found.[14] This hurts users, whose information may be stolen through a vulnerability that went unpatched because it was never reported.

The 2016 Uber breach also highlights the need for reform of the Computer Fraud and Abuse Act ("CFAA").[15] Due to the CFAA, companies are able to give white hat hackers little assurance that they will not seek civil or criminal penalties if they assist the company. The law blurs the line between ethical and unethical hacking, leaving companies and hackers in legal limbo. Former Secretary of the Army, Eric Fanning, said "what Hack the Pentagon validated is that there are large numbers of technologists and innovators who want to make a contribution to our nation's security, but lack a legal avenue to do so."[16] Last year, the Department of Justice created *A Framework for a Vulnerability Disclosure Program for Online Systems,* but following this framework only "substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law under the Computer Fraud and Abuse Act."[17] If we want white hat hackers to help companies and government identify vulnerabilities, we need to be able to give them more legal protection than they have now.

We ask that this letter be entered into the hearing record. We look forward to working with the Committee to help strengthen security practices that protect users.

Sincerely,

MARC ROTENBERG,
President,
EPIC.

CHRISTINE BANNAN,
Administrative Law and Policy Fellow,
EPIC.

Senator BLUMENTHAL. Thanks, Mr. Chairman.
Senator MORAN. Senator Cortez-Masto.

---

[10] Charlie Osborne, *Google awards researcher over $110,000 for Android exploit chain,* ZDNet (Jan. 18, 2018), *http://www.zdnet.com/article/google-awards-researcher-over-110000-for-android-exploit-chain/*

[11] Andrew Cunningham, *Starting this fall, Apple will pay up to $200,000 for iOS and iCloud bugs,* ArsTechnica (Aug. 4, 2016), *https://arstechnica.com/gadgets/2016/08/starting-this-fall-apple-will-pay-up-to-200000-for-ios-and-icloud-bugs/*.

[12] Dara Khosrowshahi, *2016 Data Security Incident* (Nov. 21, 2017), *https://www.uber.com/newsroom/2016-data-incident/*.

[13] National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 12, 2017), *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.*

[14] HackerOne, *The 2018 Hacker Report* (Jan. 17, 2018), *https://www.hackerone.com/blog/2018-Hacker-Report.*

[15] *See* Testimony of Marc Rotenberg, *Computer Virus Legislation Before the Subcomm. on Criminal Justice of the House Comm. on the Judiciary,* 101st Cong., 1st Sess. 25 (November 8, 1989) *reprinted in* Marc Rotenberg, "Computer Virus Legislation," *Computers & Society,* vol. 20, no. 1 (March 1990).

[16] HackerOne, *Hack the Pentagon, https://www.hackerone.com/resources/hack-the-pentagon.*

[17] DOJ Cybersecurity Unit, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), *https://www.justice.gov/criminal-ccips/page/file/983996/download.*

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

Senator CORTEZ-MASTO. Thank you, and thank you for this hearing. It is so appreciated. It's obviously fascinating but so needed.

Let me start, Mr. Flynn, with you because I'm trying to understand this.

So in November 2016, when you identified that data breach, at that time, were you engaging also in separate defensive bug bounty programs to help you identify security breaches?

Mr. FLYNN. Yes.

Senator CORTEZ-MASTO. And had HackerOne been on payroll already then?

Mr. FLYNN. That's correct, Senator. We had started that program in 2015, I believe.

Senator CORTEZ-MASTO. And the breach that actually occurred, was it somebody that was invited in as a defensive type of bug bounty or is this a criminal element that found a breach and exploited it to get money from you?

Mr. FLYNN. My understanding is these people came in not knowing about bug bounty programs from the get-go and it was our attempt to try to get them to use the program as it was intended.

Senator CORTEZ-MASTO. So it was a criminal element coming in to exploit and get money from you and you were trying to put them into a defensive bug bounty program to put them on the right track?

Mr. FLYNN. It's not atypical, Senator.

Senator CORTEZ-MASTO. To the panel, is that a normal process that occurs that there are some criminal elements out there, they identify a breach, they're there to exploit a company, but now we have this whole new world of bug bounty and we're going to try to put them on the right path here to help us or is it you're trying to manage somehow how much you literally have to pay out? Can I open that up? I'm just curious. This is all new to me.

Mr. FLYNN. I'm happy to answer, if you like.

Senator CORTEZ-MASTO. OK. Go ahead.

Mr. FLYNN. In my experience at least, it's not atypical to have people that come in with a report of a problem—a security issue—not knowing how bug bounty programs operate and not being familiar with the nature of the programs.

I've seen this a number of times in my career and in many cases, we can steer those people into the program and behaving in accordance with the program's requirements.

Senator CORTEZ-MASTO. Don't you have concerns that they're a criminal element? You're going to go out after them and hold them accountable because if they do it to you, they're going to do it to somebody else?

Mr. FLYNN. Well, it's not clear that they were a criminal element in the beginning of the exercise until we were able to know more about who they were and what they were after.

Senator CORTEZ-MASTO. OK. And I think I'm with Senator Blumenthal. I'm a former Attorney General. To me, that's a criminal element and you want to uncover who they are and hold them accountable and not try to somehow put some parameters around them that legitimizes them, I guess, is my concern.

Second, I'm curious about this conversation about how we have this perverse incentive and the whole idea of pricing.

Who defines that? Is it the company that actually defines that pricing cap? How does that work?

Ms. MOUSSOURIS. Well, you know, typically the organization paying will determine what price it's willing to pay. However, you know, we've seen a lot of failures to understand behavioral economics in this environment. This is not the highest bidder wins type of scenario.

Senator CORTEZ-MASTO. Right.

Ms. MOUSSOURIS. It is also not a replacement for your in-house labor costs to actually find and prevent these vulnerabilities in the first place and so when people are trying to pay for, you know, the work that it took to find vulnerability, they're missing the point. They might be able to actually better invest that money in more in-house resources to find and prevent those issues from being vulnerabilities in the first place.

The prices for vulnerabilities themselves, I think, right now, there is definitely an uptick in the pricing for various bug bounty programs. As I said earlier, that logical ceiling has to hold below a perverse incentive level.

Senator CORTEZ-MASTO. So let me ask this, and I guess we're all trying to understand whether there needs to be Federal regulation or how we address this issue so that we are putting the security protocols in place and working with vendors or people out there to help us identify it but not legitimizing a criminal element, I guess, is my concern here.

And so besides the pricing piece of this, I also understand there—I think two of you, Mr. Brookman and Mr. Mickos, you talked about that the Computer Fraud and Abuse Act, which was enacted in 1984, needs to be reformed.

Is that a venue where we can take a look at addressing all of these concerns we're hearing today, as well?

Ms. MOUSSOURIS. Absolutely. I think that, you know, providing safe harbor for researchers in the Computer Fraud and Abuse Act would go very far toward encouraging legitimate helpful hackers for coming forward because right now, it is a gray area, and especially if the scope of a program is not clear, they will not necessarily know whether they've overstepped and they might be afraid to come forward.

So we want to encourage that. We want to provide safe harbor for them in the form of reforms to the Computer Fraud and Abuse Act because the actual act of discovering vulnerabilities for defense and discovering them for exploitation purposes, those are technically indistinguishable acts.

Senator CORTEZ-MASTO. Right.

Ms. MOUSSOURIS. So providing that safe harbor is going to be important.

Senator CORTEZ-MASTO. OK. And I know my time is up, but this is a fascinating topic. So I appreciate it.

Mr. Brookman, I didn't know if you had a comment quickly on any of this.

Mr. BROOKMAN. Yes. I would not encourage Congress to try to micromanage the bug bounty process. I did not testify about to see

if they would reform, though I certainly am sympathetic to a lot of the issues you talked about.

But as I stated in my oral testimony, I think the most important thing you can do is shift the incentives to the companies that do bear the costs of data security incidents, you know, whereas we're seeing, you know, companies, like Equifax, will have a stock hit and then like, you know, a year later, they're back to where they were. They're not bearing the cost of that identity theft.

You know, some companies who are hit a lot do have good robust programs but you see that a lot of the top companies, I think, you know, systematically in the industry, you don't see enough of this. So the incentives need to change.

Senator CORTEZ-MASTO. Thank you. Thank you very much.

Senator MORAN. We're going to have a second round. Let me start by asking this question.

When, if ever, is it appropriate to disclose a cyber security vulnerability to the public before it's fixed?

Ms. MOUSSOURIS. So having run Microsoft Vulnerability Research, which was an organization within the Microsoft Security Response Center, designed to notify other parties of either vulnerabilities we found ourselves internally that affected third party software, and it was also a coordination arm that would coordinate among multiple parties, so think of the, you know, multiparty coordination involved with Heart Bleed or with the Meltdown Inspector incidents.

There are times when a vulnerability in question affects so many different organizations that you may do the best you can to coordinate the activities of creating patches all up and down the supply chain but you will inevitably have to leave some out of the embargoed disclosure, the staged disclosure of these vulnerabilities, which means in the end, you will be doing the best you can to prepare as many organizations as possible, but you will end up disclosing a vulnerability before everyone has had a chance to either create patches or apply some of the patches that you've created.

So that is one example of a legitimate circumstance where you would disclose ahead of a patch. Another is simply that there is exploitation going in the wild, a patch isn't ready, and you need to disclose to warn users and administrators to be able to mitigate and protect themselves.

Senator MORAN. Before anyone else responds, let me turn to Senator Blumenthal, who has to return to Armed Services.

Senator Blumenthal.

Senator BLUMENTHAL. I have a classified Armed Services briefing or hearing that I have to return to, but I just want to highlight one of the comments I made at the beginning.

Without casting aspersions personally on anybody here, I hope that you would agree that stronger legislative tools have to be given to the Federal Trade Commission. I hope that you will work with me on the Data Breach Accountability and Enforcement Act of 2017 which the Ranking Member and I have co-sponsored.

The FTC needs tools to adequately protect consumers and to prevent future damaging breaches. So that's a final request. I hope that you are sympathetic to it and that you will support efforts to move forward with those kinds of tools.

Thank you, Mr. Chairman, and I apologize that I'm going to have to take off.

Senator MORAN. Thank you very much, Senator Blumenthal.

Let me ask this question to Mr. Flynn. The Justice Department published a set of guidelines aimed at helping companies run bug bounty programs within the law. These guidelines included a suggestion that any firm inviting hackers into their systems consider imposing restrictions on a hacker "accessing, copying, transferring, storing, using, and retaining" sensitive data.

As of last Friday, February 1, Uber had not added such a clause to their Bug Bounty Program listed on the HackerOne website.

Does it have plans to add a similar clause to its policy? If this type of clause had been included in Uber's program, how would a bounty request in the 2016 breach have been treated?

Mr. FLYNN. So let me first say I think it's a great point. We are going through that process right now of looking at our clauses exactly as you describe. I'm not a lawyer, so I can't really speak to the details of the clause itself, but I think it's a great suggestion, and I think I'm going to take it back and have a discussion about it with my team.

And then you had another question at the end there, if I recall.

Senator MORAN. I just wondered how different it would have been in 2016 if that clause had been a matter of practice?

Mr. FLYNN. I think the answer I would imagine is, you know, essentially this was not a typical bug bounty situation, as I described, and I would say that, you know, I think there was a real attempt to try to get this individual to participate in the program, but ultimately this person was, you know, offering extortionist demands and so I think, you know, looking back on it and learning what I've learned now, I think the better approach would be to have a separate process once you determine that it's outside of the scope of the program itself and engage that process at that time.

Senator MORAN. Thank you very much.

Mr. FLYNN. Yes, you're welcome.

Senator MORAN. Senator Blunt.

STATEMENT OF HON. ROY BLUNT,
U.S. SENATOR FROM MISSOURI

Senator BLUNT. So, Mr. Flynn, when Uber has somebody get inside their system, did I understand that that would be their records on where every driver drove and every rider rode and maybe their entire rider history? Is that the kind of thing you would see if you got into your system?

Mr. FLYNN. So in this case, Senator, this was a backup of a very specific database stored outside of our systems and the data that was stored there did not include the elements you described. It included—it had a number of records for—I think it was, you know, 25 million different users, but of——

Senator BLUNT. Would it have had the payment records for those users?

Mr. FLYNN. It had credit—sorry. Excuse me. It had—sorry. Let me just look here. It had the drivers' license numbers for 600,000 of our drivers included in that data store.

Senator BLUNT. What else did it have, besides that?

Mr. FLYNN. It had—for new e-mail users, it had the names, e-mail addresses, and phone numbers of those users. For some of the users, it had Salton and Hash passwords. It didn't include some of the things you described, trip location history, credit card information, bank account numbers, plain text passwords, social security numbers, or birth dates. Those were not included in the data.

Senator BLUNT. And what have you done since then to secure that data in a better way?

Mr. FLYNN. Well, within 24 hours of learning about this incident back in 2016, we took a number of important steps: the first of which was, you know,—so just describing the attack briefly, the attacker got into an external GitHub repository, which had some of our source code, by using a password of one of the users that was in the system.

We rotated all the passwords. We implemented multi-factorial authentication on the system. The attacker also took advantage of finding keys in the code base that was stored in that infrastructure. We rotated all the keys and actually put them in a secure storage system, as well, and, finally, the keys that the attacker was able to glean from that code repository was then able, in turn, to be used against our Amazon S3 external infrastructure.

We also rotated the keys, put them in a secure storage location, and we put IP-based restrictions on those keys so that they couldn't be used to access that data going forward.

Senator BLUNT. For those of you who worked to find flaws in the system or protect a system, what kind of lessons would be learned there from the ability to get to that information?

Mr. Mickos, is that what you do?

Mr. MICKOS. Yes, Senator Blunt, we are a platform that connects the hackers to the companies. We do not look for vulnerabilities ourselves or fix them, if that was your question.

Senator BLUNT. Yes. So you do not do that. Do you provide the platform?

Mr. MICKOS. We provide the platform and, if you will, the marketplace between the two and we provide a trusted place where hackers can trust that they will be well treated by the customers, the companies, or government organizations, and they in turn can trust that they know who they're dealing with on the hacker side. That is our business.

Senator BLUNT. And I'm assuming your name is not Missouri?

Mr. MICKOS. No. My name is Mickos.

Senator BLUNT. No. Yours is Mickos. What is your last name?

Ms. MOUSSOURIS. My last name is pronounced Moussouris or at least that's how I've——

Senator BLUNT. I was close.

Ms. MOUSSOURIS.—chose to mispronounce it.

Senator BLUNT. I was pretty close. Half of the people where I live call our state Missoura and half call it Missouri and——

Ms. MOUSSOURIS. You miss——

Senator BLUNT.—you could easily mistake your name.

Now what—from your company perspective, what lessons should we learn there?

Ms. MOUSSOURIS. Well, my company actually does help organizations look at their overall defensive picture and helps them figure

out the best way to work with the hacker community but actually looks at their business goals when it comes to security.

So in terms of the trusted advisorship, when we look at their capabilities, we look at whether or not they're actually actively investing internally on some operational security basics, such as what would have prevented, you know, this type of breach where keys and credentials were available.

There's a lot you can do in terms of low-risk internal investments in terms of security, which have been documented by, you know, lots of organizations over the past 25 years of developing information security best practices.

So we don't just advise on how to start a bug bounty. It's really about looking at the overall picture, looking at where your investments are, and determining is it actually a place where you can invest further on your internal staff, further in terms of operational security, and then prepare the mechanisms such that you can receive vulnerability reports from the outside, whether it's from a hacker or from one of your suppliers.

I mean, this really could be from anywhere. It could even be from the Federal Government letting you know that you have a vulnerability. So it's building capacity.

Senator BLUNT. And, Mr. Brookman, is there a growing concern about how much information is out there and how many people seem to be able to get their hands on it?

Mr. BROOKMAN. Yes, certainly. I mean, as I testified, data breaches are commonplace for people. Companies don't have sufficient incentives. I mean, we've seen in so many of these hacks and there are things that maybe, you know, it's easy to play Monday morning quarterback, but things that were easily remediable.

In this case, hard coding AWS of credentials in GitHub is an incredibly common practice, one that Uber had been caught doing before. It was a private account but still generally considered not to be best practice.

Equifax case, updating the website to address the publicly known vulnerability. Even the companies that are trying to do it right get it wrong and there's just not enough incentive for companies to try to get it right.

Senator BLUNT. Thank you, Chairman.

Senator MORAN. Thank you, Senator Blunt.

Senator Cortez-Masto.

Senator CORTEZ-MASTO. Thank you. I have one final question.

Small businesses, you know, in Nevada, there are probably almost 240,000 of them. The conversation I have with them all the time is their cyber security and they just don't have the resources to really address this issue and are oftentimes victims.

Any thoughts on what can be done to help our small businesses and give them the tools they need to protect their cyber security? And I would just open it up to whoever. Mr. Mickos, Ms. Moussouris.

Mr. MICKOS. Yes, Senator Cortez-Masto.

Senator CORTEZ-MASTO. Yes, please.

Mr. MICKOS. As I said in my opening statement, we believe, as DOJ and others, that a vulnerability disclosure program is useful for anybody. This is what then Secretary of Defense Ash Carter

said. "If you see something, say something," meaning every company with software that contains valuable consumer data, they need to have an ability to receive input from the outside world because there's so much good intent among security researchers and hackers on the outside.

And I would recommend you to read this report, the 2018 Hacker Report where we go through the hackers and what motivates and how they work.

So back to your small businesses, if they will have a way of receiving vulnerability reports and taking action, they will all successively get more and more secure.

Now to be a little bit more specific, many of them, of course, don't have IT staff. They are working with a third-party provider where they run their website or mobile application. That provider has a very important responsibility in doing the same.

Senator CORTEZ-MASTO. OK. Thank you.

Ms. MOUSSOURIS. So I would say that, first and foremost, the small businesses need to run some of these freely available tools on their own infrastructure before they invite external parties in to do so.

Doing so first is just part of their own preventative mechanisms. That will give them a decent picture before they operationalize what I very strongly support, which is having vulnerability disclosure programs, but you need to be able to take care of the bugs you already know about yourself first.

The fact of the matter is, it's not just small businesses that have a problem dealing with vulnerabilities they already know about. There's been a doubling in the common vulnerabilities and enumeration where the CDE count, the overall bug count, that have been reported.

There was a doubling last year of reported vulnerabilities. There is a bug fatigue that is plaguing organizations and governments all over the world and it is not just small businesses.

So we have an operational problem and I think that preventative measures and looking internally first, growing those capabilities, and then looking to outside help is the way to go.

Senator CORTEZ-MASTO. Thank you.

Mr. BROOKMAN. I just had a couple thoughts. This is fantastic question. I mean, when you look at, you know, companies, like Uber, who have invest in the best and the brightest, even they have problems.

I think a few words of advice. One, practice data minimization. I mean don't connect stuff you don't need to be connected. Don't collect data you don't need, get rid of all data. A general recognition to try to update everything. I mean, you rely on vendors, nonupdated software is one of the biggest problems in this space.

The FTC has some really good resources on this with their Start with Security series, which I know you contributed to. It's really fantastic guidance for small businesses in this area, so I would point people to that.

Senator CORTEZ-MASTO. Thank you. Thank you very much. I appreciate the panel and the discussion today.

Senator MORAN. Senator, thank you very much.

Let me ask a final question and then we'll conclude this hearing.

You're all aware likely that 48 states have different data security breach notification laws. This patchwork creates a different standard, depending on where you are, and many companies, as we know, operate outside of a state and they contract with people who are in different places to do their security work.

Anyone have any thoughts about Federal preemption legislative solution in regard to notification so that there's greater clarity and certainty for a company in their obligations?

Mr. FLYNN. Senator, if you might, if you don't mind, as a defender and having dedicated my life to protecting customer data and implementing security engineering defense, I would say that it is something I would very much support personally because I do believe it's very hard for companies to contend with this patchwork of notification regulations throughout the United States.

So, Senator, a short statement, but I believe very much that this is the right approach and I'd love to work with you on it, if I can.

Senator MORAN. Thank you.

Mr. MICKOS. Mr. Chairman, as I said in my opening statement, we're in support of this. I would love to work with you on the details of such legislation.

Senator MORAN. Thank you.

Mr. BROOKMAN. I would say I have significant reservations about that. I mean, if the approach of a Federal bill is just to make it simpler to have a data breach incident, then that, you know, decreases an incentive and decreases their costs and I think could lead to actually a worse security environment.

I would encourage any statute to allow states to actually pass new bills, especially for information that's not covered.

In my opening statement, I mentioned e-mail accounts, photo storage accounts, not originally in data breach notification bills, but over time people have recognized, well, there's some really sensitive stuff in there. If my iCloud gets hacked, I should be told about it. I would not want to see a Federal bill say, OK, here are the 18 elements that you need to be notified for and then prevent the states from over time changing that.

I mean, we can discuss other ways to update it over time, give the FTC the ability to nullify the definitions, but I'd be very nervous about freezing that in time with Federal legislation.

Ms. MOUSSOURIS. And I would say that, you know, I look forward to helping to contribute to make sure that any kind of legislation that normalizes data breach laws takes into account that we don't want to create an environment where organizations are incentivized not to know and not to detect, to avoid data breach laws.

We don't want to swing the pendulum backwards and so I look forward to working with you as this goes forward to not create some of those unintended consequences of over-legislation.

Senator MORAN. We welcome all of you on working with us, but especially intending to avoid unintended consequences.

Is there any witness who would like to add anything to the record before I close it out? Anyone have something they'd like to make certain is said before we conclude the hearing?

[No response.]

Senator MORAN. Thank you very much.

Then 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.

This concludes our hearing today, and I'm very grateful to our witnesses.

We are adjourned.

[Whereupon, at 4:10 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO JOHN FLYNN

Question 1. What separates a good faith researcher from a malicious actor? What's to stop a criminal from posing as a researcher? How can companies or vendors tell the difference?

Answer. A good faith researcher investigates and discloses vulnerabilities in an ethical manner consistent with the prescribed terms of the bug bounty program. Good faith researchers are generally cooperative throughout the bounty process and willing to abide by the program's rules. Although it may not always be apparent what someone's intentions are or whether a criminal actor is posing as a white hat researcher, certain conduct should raise a red flag. Anyone who in bad faith strays beyond the bounds of the bug bounty program by engaging in behavior such as maliciously compromising user data, making threats, or making extortionate demands should not be considered a good faith researcher.

Question 2. What is the role of bug bounty programs when faced with extortion attempts?

Answer. Bug bounty programs are designed for good faith researchers, not extortionists.

Question 3. As you have acknowledged, the hackers involved in the 2016 breach of your company did obtain data of your users. As it relates to Uber's specific bug bounty program, how often is data actually obtained by the hacker that is disclosing a vulnerability to your company? Was the sheer number of exposed and obtained records in the 2016 case unusual compared to other vulnerability disclosure cases your company had witnessed through the bug bounty program?

Answer. Most often researchers will use test accounts or access their own data when researching vulnerabilities. If the researcher comes in contact with user data while acting in good faith, the access should be limited to the minimum amount needed to identify and report the vulnerability. We agree that the 2016 incident was unusual compared to other vulnerability disclosure cases witnessed by Uber in terms of sheer number of records.

Question 4. HackerOne's 2018 Hacker Report and a 2016 study conducted by the National Telecommunications and Information Administration (NTIA) both indicated that profit is a relatively limited motivation among hackers participating in coordinated vulnerability disclosure programs. Given the panel's experience with professionals in this field, could you please further describe the predominant motivators.

Answer. Historically, before there were bounty programs, researchers would report vulnerabilities as a way to build their reputation in the security community and among their peers. Even today this is the biggest motivator and can open doors for researchers, such as being offered jobs to work for the companies whose vulnerabilities they uncovered.

Question 5. Would you agree that it is absolutely critical for companies to administer any vulnerability disclosure program responsibly based on sound principles (such as those included in DOJ's 2017 guidelines) as it has obvious impacts on industrywide use of these types of programs that are proven to protect consumers?

Answer. Yes. Bug bounty programs are critical for many large companies to detect security issues, and the programs should be designed and managed responsibly so that they can continue to be an important security tool. The DOJ's 2017 framework is a good starting point. It is not prescriptive, but rather outlines a process that companies considering bug bounty programs can follow to clearly define for researchers what the company considers to be authorized vulnerability disclosure and discovery conduct.

Question 6. Did Uber have a predetermined maximum bounty amount for its bug bounty program? If so, what was the maximum amount?

Answer. Uber's Bug Bounty program at HackerOne has a published maximum payment of $10,000, see *https://hackerone.com/uber,* but the actual amount of any payment under the program is up to Uber in its sole discretion, see *https://www.uber.com/legal/other/bugbountyprogramterms/* ("Bounty payouts, if any, will be determined by Uber in its sole discretion.").

Question 7. Mr. Mickos's testimony stated that the Computer Fraud and Abuse Act is in need of modernization to prevent liability of hackers acting in good faith in identifying vulnerabilities to protect consumers. Do you have any specific recommendations related to modernizing the law?

Answer. Other panel participants are closer to these issues, but we at Uber understand that those speaking on behalf of good faith security researchers would like to see more clarity that when conduct complies with the terms of a bug bounty program, it is not "unauthorized" access under the Computer Fraud and Abuse Act.

Question 8. Following an inquiry that I sent along with Chairman Thune and our colleagues from Senate Finance Committee, Uber responded with a letter on December 11, 2017, describing the 2016 breach and the ensuing actions taken by the company. The letter described the payment of $100,000 to the two individual hackers responsible for the breach and stated, "It thereafter engaged in further communications with the two individuals using their real identities, including having them sign assurances that the data was destroyed." For the sake of clarity, was the $100,000 paid to the two individuals prior to their real identities being known?

Answer. As I explained in my written testimony, I was not part of the "attribution" team—the team that determined the two individuals' real identities. I was aware that the process of paying them was part of the process of determining their identities, but I am not sure if their identities were confirmed prior to or after the moment the payment was made.

Question 9. Please describe to the greatest extent possible the "assurances" that were made to Uber's "attribution team" that the stolen data had been eliminated. Were signed documents the sole source of assurance?

Answer. It is my understanding that the attribution team obtained various sources of information about the destruction of the data, in addition to the signed documents and in person meetings.

Question 10. Please describe the measures Uber has taken to confirm these assurances and monitor the affected accounts for additional fraud protection.

Answer. We have seen no evidence of fraud or misuse tied to this incident. That being said, we have identified the 57 million affected accounts in our systems, and have tagged them for a heightened level of fraud protection. Specifically, we have created new fraud "rules" that will surface any unusual activity on the accounts going forward. Uber already looks at many signals like location or device ID, in addition to e-mail address and password, to authorize logins to Uber user accounts. Additionally, we automatically send users a second factor authentication request such an SMS or e-mail if we detect a high-risk login attempt.

Response to Written Questions Submitted by Hon. Brian Schatz to John Flynn

Question 1. Uber has argued repeatedly that it is a tech platform, rather than a transportation company. By using this characterization, the company is able to avoid certain local and Federal regulations that protect consumer safety and worker rights. But last year, Uber made a deal to purchase and deploy 24,000 autonomous vehicles from Volvo. Is Uber a transportation company or a tech platform company? For cybersecurity, whose rules and standards does Uber follow at the Federal level?

Answer. Uber is a technology company and not a transportation company. It is a technology company that strives to make a difference in the lives of people in the real world, starting—for now—with improving how transportation resources are utilized by matching drivers with riders (the Uber app), shippers with haulers (Uber Freight), and consumers with restaurants and restaurants with delivery partners (Uber Eats). Uber's technology creates and standardizes markets that efficiently connect otherwise unmatched supply and demand, but Uber itself is not a participant in the market.

At the Federal level, the Federal Trade Commission regulates data security for consumer-facing technology services through Section 5 of the FTC Act. In addition, some specific aspects of Uber's services are subject to applicable sector-specific laws, such as HIPAA.

Question 2. In your written testimony, you state that Uber is "working to make transparency and honesty core values of [the] company." What specifically has Uber done to increase transparency and make honesty part of its core values?

Answer. Uber has taken several steps to ensure that transparency and honesty are core values of the company. First, Uber created a robust Integrity Helpline for its employees to report concerns. Second, Uber has also embraced all of the recommendations presented to it by former U.S. Attorney General Eric Holder regarding improving Uber's workplace culture. Third, it is devoting resources to improve and expand its Compliance team. Fourth, it has installed additional safety features for riders and drivers in its app. Finally, Uber now gives victims pursuing individual sex assault or sex harassment claims the choice to litigate their claims in court or arbitration.

Uber is not perfect, but it is deeply committed to being better and to doing the right thing, and it will continue to engage in the self-reflection and change that are essential to getting where it wants to go as a company.

Question 3. What percentage of Uber's annual revenue and workforce are dedicated to minimizing the risk of future data breaches outside of a bug bounty program? What were those percentages before the 2016 data breach?

Answer. Uber has long devoted substantial resources to minimizing the risk of data breaches, separate and apart from its bug bounty program. Some of these other efforts were noted in Uber CISO John Flynn's written testimony to the Subcommittee, which explained at page 2 that bug bounty programs are just one part of a comprehensive data security program. Uber's internal work efforts to minimize the risk of data breaches is, in many respects, part and parcel of other aspects of quality code development since minimizing vulnerabilities is a component of writing high-quality code, and it is also a part of broader security efforts relating to all aspects of security including physical security as well as data security. As a result, it is difficult to quantify the percentage of Uber's annual revenue and workforce "dedicated to minimizing the risk of future data breaches outside of a bug bounty program," and that is not a metric that Uber keeps in the ordinary course.

Question 4. Other than the 2016 data breach, how many other incidents has Uber experienced where cyber intruders extorted the company?

Answer. The team at the company that handles cybersecurity threats is not aware of any other incidents in which a cyber intruder extorted the company.

Question 5. What exactly did Uber get in exchange for paying the extortionists $100,000 through HackerOne? Did Uber confirm that the data was deleted? How did Uber make this confirmation?

Answer. Uber paid the outside actors $100,000 in exchange for their agreement to delete the data they had downloaded and their written and oral assurances that they had destroyed and would not use or disseminate that data. The process of making the payment also helped to determine the real identities of the outside actors, which enabled Uber to engage in further communications with them regarding technical details of how they had deleted the data. Uber has seen no evidence that the data downloaded by the outside actors has been disseminated or used, or any evidence of fraud or misuse tied to this incident, since the incident occurred over a year ago.

Question 6. What policy changes has Uber enacted in response to the 2016 data breach?

Answer. Uber has taken several steps in response to the 2016 data breach. At the time of the incident, Uber determined the means of access, shut down the credential used by the outside actors, and took other steps intended to confirm that the outside actors had destroyed and would not use or further disseminate Uber's data. Uber also imposed technical security measures designed to prevent a similar incident from occurring in the future, as described on page 6 of Uber CISO John Flynn's written testimony to the Subcommittee; these technical improvements are now a part of Uber's baseline security posture. Additionally, Uber has made a number of policy changes since the incident including the following:

- Uber adopted specific written policies to establish baseline security measures that are required for use of Amazon Web Services and S3.
- Uber revised its Bug Bounty program terms, specifically to provide more detailed information about what type of conduct is not good faith conduct and what the limits are on accessing user data.
- Uber is revising its incident response plans.

Question 7. Does Uber have an internal whistleblower program? How is it managed?

Answer. Uber's Integrity Helpline is available to all employees for reporting concerns. Employees may report their concerns to the Helpline via website or telephone in their language of choice. The Integrity Helpline is hosted by an independent third-party to ensure the anonymity of the reporter, if desired by the reporter, and is maintained by Uber's Global Compliance team. Upon filing a report, the reporting employee will be provided with an access code to use so that she or he can contact the Integrity Helpline to track her or his report. Once a report is filed, it is sent to the relevant Uber team for review and investigation, and appropriate action will be taken for substantiated reports.

Question 8. In March 2015, Vice News reported that stolen Uber accounts were being sold on the dark web for $1, although Uber claimed that there was no data breach at the time. To Uber's knowledge, how was this account data stolen? How many data breaches have been occurred at the company? Does Uber keep an estimate of how many stolen accounts are sold on the dark web? What is the current estimate? How many complaints does Uber get from customers per month about stolen accounts?

Answer. As indicated in the original Vice article that we believe is referenced by the question (*https://motherboard.vice.com/en_us/article/z4mk7j/stolen-uber-customer-accounts-are-for-sale-on-the-dark-web-for-1*), Uber found no indications that it suffered a data breach. Indeed, the article itself merely claimed that it found Uber account login information available for sale, but acknowledged that while "[t]hese logins may indicated that Uber's security was hacked or compromised somehow . . . [*i*]*t also might mean that these customers were breached individually by other means, and their Uber credentials harvested and put up for sale.*" (Emphasis added).

Given that Uber found no evidence of a data breach that could have led to the login information for these accounts being stolen, it has no non-speculative information about how the information was obtained. As one possibility, when people choose to use the same or very similar login credentials for multiple online or app accounts, or simply use easy-to-guess passwords, third parties can sometimes determine those credentials. These types of "account takeovers" are a common problem across all online services, Uber as well as others. Uber addresses the issue as described in the response to the next question, below.

Question 9. How does Uber address stolen accounts? Please walk through the experience that a typical customer would go through when he or she notices suspicious account activity. How does a customer resolve issues with a stolen account if the thief has changed the e-mail address or phone number associated with the account? How effective is Uber at resolving customers' complaints about stolen accounts.

Answer. Uber takes reports of fraud very seriously, regardless of their root cause. In the United States, when Uber detects a suspicious login to an account, even if the user has not notified Uber of concerns, Uber sends a second-factor authentication request to the user to help stop and prevent the incorrect person from accessing the account. When a rider notifies Uber about suspicions that his or her account has been stolen or taken over, Uber's customer support representatives: (1) will look for signs that the account has been compromised, (2) secure the account by rotating the user password and forcing two-factor authentication, (3) restore the account (*i.e.,* reverse any changes made to the user's e-mail, phone number, etc.), (4) refund the affected rides, and (5) advise the user about the risks of password re-use. The process for drivers is similar, except drivers must verify that their payment information is correct before Uber unlocks their account.

Question 10. Uber recently signed onto the Shared Mobility Principles for Livable Cities—one of these principles is in support of open data. But, citing user privacy issues, Uber has not always been successful in sharing data with local planning officials. User privacy is important, but so is sharing data with cities. How exactly will Uber now prioritize meaningful data sharing with state and local governments? Where is the sweet spot between user privacy and providing data to city planners and other government officials?

Answer. Uber is committed to building replicable models for sharing insights with city planners and other government officials. Last year, we launched Uber Movement, a free and public website using Uber's data to help cities address some of the challenges they face day to day. We engaged with city leaders, urban planners and civic community stakeholders around the world to validate our assumptions to develop and design Movement. Right now, Movement is optimized to look at macro trends in a city to accommodate specific urban use cases—traffic analysis and demand modeling and also understanding the impacts of different infrastructure investments and changes to the built environment—road closures, bridge closures, etc.

Additionally, we're working with the non-profit SharedStreets to create new methods for public-private collaboration and data sharing that respect the need for rider

and driver privacy as well as the competitive landscape of the industry. We're starting with a pilot in Washington, D.C., and are working with the District Department of Transportation, Department of For Hire Vehicles, and SharedStreets to share data on curb usage across multiple modes of transportation. Better understanding curb utilization can help cities around the world prepare for a future where more and more of us are accessing transportation through a combination of shared modes, rather than relying on our own vehicles. We're looking forward to building on what we learn from working with DC to support data partnerships in other cities using SharedStreets data standards.

Earlier this year, we also announced the Cincinnati Mobility Lab, a first-of-its kind multi-year partnership with the City of Cincinnati to explore different mobility issues. Through this partnership, we're sharing insights that look at how to improve the problem of curb congestion, to commuting challenges, to working to develop a strategy for the future of the City's public transit service—one that is seamlessly integrated with other ways of getting around the City.

Question 11. Uber often touts the potential for transportation network companies to complement public transit by providing the last-mile service. Does Uber currently provide those services to riders with small children who require car seats or does it require customers to provide appropriate safety equipment? Does Uber currently provide those services to riders with a disability or limited mobility? Does Uber currently provide those services to older adults or persons with limited technology proficiency? What accommodations does the company make for those groups? Does Uber levy additional charges on those riders?

Answer. Riders and drivers using the Uber app are expected to follow local laws when it comes to transporting infants and small children. In certain locations, for an additional fee, people who ride on the Uber app can request a vehicle equipped with a car seat. The seat is forward-facing and for children who are at least 12 months old, 22 lbs, and 31 inches tall. Additional details about the car seat offering can be found here. People who ride also have the option to bring their own seats for installation in Uber. However, it is up to the person driving to accept the trip and they may cancel the trip if they so choose.

Uber works hard to understand the needs of elderly riders and riders with disabilities. For example, the uberASSIST option in the Uber app is designed to network riders who would like a helping hand with drivers who have chosen to obtain training from a third-party organization on how to provide additional assistance. In addition, we developed the Uber Central dashboard to allow senior centers and other organizations to call rides for senior riders who may not have access to a smartphone. Finally, the "Request for a Guest" feature allows Uber users to seamlessly request a ride for their loved ones right from the Uber app. The senior receives a text message with the vehicle information and the driver's phone number so they can communicate directly with them.

Additionally, the Uber app is compatible with various accessibility technologies, including VoiceOver, TalkBack, and wireless braille (depending on hardware and operating system) that can help provide a safe and reliable transportation option for the blind and low-vision community. In addition, by providing visible and vibrating alerts as well as GPS navigation, Uber has provided economic opportunities for drivers who are deaf and hard of hearing. Both the Uber Rider and Driver apps are monitored and tested regularly by internal resources and by a third-party provider of Accessibility testing and monitoring. You can read more about our Accessibility efforts on our website here: *https://accessibility.uber.com/*.

All driver-partners are expected to accommodate riders using walkers, canes, folding wheelchairs, service animals, or other assistive devices to the maximum extent possible. Where available, UberWAV lets riders who use non-folding, motorized wheelchairs to connect with drivers in wheelchair accessible vehicles that are equipped with ramps or lifts.

Question 12. When providing the last-mile service, how does Uber ensure that cars are available in all areas of a city at all times? How does Uber provide access to riders with limited or no access to the Uber app?

Answer. By design, our app aims to make efficient and reliable transportation a possibility for everyone, everywhere. Our technology automatically and efficiently matches riders' requests with nearby drivers, and real time dynamic pricing ensures that the supply of cars can meet the demand from passengers. As Uber has grown, more people in more parts of cities have been able to push a button and get a ride. Over time, wait times have decreased significantly across more parts of cities, including parts that other means of transportation cannot reach. In Los Angeles, a metro area that covers 100 square miles, the average ride is less than 10 minutes away, and in New York's outer-boroughs, riders are just as likely to get picked up

as if they were in downtown Manhattan. In fact, a majority of our trips in New York now start outside Manhattan and 52 percent don't start or end in the central business district.

As mentioned in our response to Question 11, the Uber Central dashboard allows organizations, like senior centers or transit agencies, to call rides for riders who may not have access to a smartphone. Additionally, the "Request for a Guest" feature allows Uber users to seamlessly request a ride for their loved ones right from the Uber app. The senior receives a text message with the vehicle information and the driver's phone number so they can communicate directly with them.

Question 13. Uber recently signed onto a letter with the Service Employees International Union supporting portable benefits. What benefits is Uber planning provide to its drivers? Will they be offered nationwide?

Answer. Uber's joint letter with the SEIU and Civic Venture Partners is about working together on the creation of a portable benefits system in Washington state. We are working with our partners, the business community and labor to make progress on this important policy goal with a view to determining policy and regulatory frameworks over the course of 2018 and developing legislation for introduction in 2019. We would be eager to provide your staff updates as this effort progresses.

While we continue our work in Washington state, we are working to provide additional benefits to our drivers nationwide. For example, we believe that at a basic level everyone should have the option to protect themselves and their loved ones against rare and unforeseen work accidents that prevent them from earning a living. That is why Uber, with Aon, now enables drivers to access a driver injury protection program for a few cents per mile directly through the Uber app. This product provides Uber driver-partners the option to obtain coverage for medical expenses, disability payments and a survivors benefit resulting from a covered accident. Drivers who elect to enroll are protected for injuries while online, en route and on-trip in connection with the Uber app; however the premium of a few cents per mile is calculated and charged only for miles travelled while on-trip.

While the Driver Injury Protection insurance offered to Uber's driver-partners is first-of-its-kind, it is the latest example of benefits designed primarily for independent workers. In the US, Uber's partnership with Betterment enables drivers to contribute to their retirement savings, while 150,000 drivers have been able to navigate the healthcare market through Stride Health.

Drivers can also file their taxes and claim returns through our partnerships with Stride, TurboTax and H&R Block, cash out their earnings instantly with Instant Pay, and receive discounts on fuel and other operational expenses.

Question 14. Uber has repeatedly admitted to underpaying its drivers. What oversight has Uber put in place to ensure that this does not happen again?

Answer. We have made an effort to regain drivers' trust by owning up to our mistakes and improving the driver experience from end-to-end. In particular, we have made many improvements for drivers designed to make their earnings easier to understand and access, including:

- *Easier to understand rates*—Drivers see the exact rates they earn for every minute and every mile they drive. Previously, drivers needed to deduct Uber's service fee from their rates to determine their earnings. Now, no math is required. Drivers will always know exactly what they'll earn.
- *Clearer in-app earnings pages*—In response to driver requests for more clarity in our earnings calculations, we have updated our trip receipts. Drivers now see a clear breakdown of how their trip earnings were calculated, as well as additional fare details, including what the rider paid and Uber's service fee.
- *Faster fare receipts*—Drivers tell us seeing what they earn in real-time is important. We have committed to a goal of having earnings details available in the app within 15 seconds after a trip ends.
- *Cash out more earnings, anytime*—With InstantPay, drivers are able to cash out their earnings (including promotions) instantly up to five times a day. We've made promotions available for immediate cash out through Instant Pay.

Additionally, we have defined new policies and controls designed to help ensure drivers earn what they are owed for every trip. We also have a dedicated, cross-functional oversight group tasked with reviewing and approving all pricing and service fee changes.

Question 15. Uber has committed to changing its workplace culture to address discrimination and sexual harassment concerns. What policy changes have been en-

acted for full-time, permanent employees of Uber? What policy changes have been enacted for drivers of Uber?

Answer. Uber is not immune from the global epidemic of sexual violence, which affects nearly one in three women worldwide, and we want to be a big part of the solution. That's why we've committed to making important changes. Over the last year, we've met with 80+ women's groups and have been working closely with advocates and experts from sexual assault organizations to listen and incorporate feedback about how we can make a difference.

Experts tell us that one of the best ways to prevent sexual harassment incidents is through education and awareness. That's why we've committed $5 million to support prevention initiatives, and have been partnering with leading organizations in this space to educate our employees, riders and drivers with important information on this topic.

We recently made important changes to give victims of sexual assault and sexual harassment more choices, ensure they have the option to share their story, and raise the bar on transparency:

- First, Uber no longer requires mandatory arbitration for individual claims of sexual assault or sexual harassment by Uber riders, drivers or employees. We believe the survivor should choose their venue of redress for their individual claims, whether that's in court or arbitration.
- Second, survivors now have the option to settle their claims with Uber without a confidentiality provision that prevents them from speaking about the facts of the sexual assault or sexual harassment they suffered. The decision to talk about what happened should rest with the survivor, not Uber, and supporting that choice will help end the culture of silence that surrounds sexual violence.
- Third, we committed to publishing a safety transparency report that will include data on sexual assaults and other incidents that occur on the Uber platform. We are the first ridesharing company in the world to make this commitment.

In addition, we believe that sexual assault awareness should permeate every level in our company. That's why we have begun educating employees—starting with our executive leadership team, who receive training on sexual assault and sexual harassment prevention hosted by experts from the National Alliance to End Sexual Violence and the National Network to End Domestic Violence, and we'll continue to do more. We have a robust HR team and systems equipped to handle and manage a myriad of employee matters, and we have an anonymous hotline where anyone can bring their workplace issues. Our Employee Relations team, solely dedicated to investigating and addressing employee issues, has been strengthened. We've also taken the following steps to improve our culture: performance review system, compensation review, manager trainings, Executive Education, $3M diversity fund, improved hiring practices to promote diversity & inclusion. Additionally, we implemented a comprehensive equal pay analysis and have ensured aggregate pay equity between women and men, and between all racial groups.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO MARTEN G. MICKOS

Question 1. What separates a good faith researcher from a malicious actor? What's to stop a criminal from posing as a researcher? How can companies or vendors tell the difference?

Answer. Intent is what separates a good faith security researcher from a malicious actor. Researchers that are reporting vulnerabilities through lawful channels are doing so with the intent that the vulnerability report be delivered to the owner of the system for the bug to be resolved.

Vulnerability disclosure and bug bounty programs are so designed that they provide no particular benefit or special access to the participants. On the contrary, the programs generate additional work for the participant while collecting various pieces of information about them. For these reasons, a malicious actor has something to lose and nothing to gain in such a program. It is more rational for the malicious actor to engage in their unauthorized activity outside of the program.

Like in most professional endeavors, it is at least in theory possible for a criminal to pose as a legitimate participant. But given that there are no benefits but only obligations in a program, this would not be rational behavior. The only way to receive a benefit from a vulnerability disclosure or bug bounty program is by reporting a valid vulnerability to the owner of the system. When that happens, a vulnerability can be removed and rendered unusable by criminals.

Criminals, for the above mentioned reasons, do not wait for vulnerability disclosure or bug bounty programs to start, and they obtain no benefit from joining such programs if they exist. Criminals engage in their unauthorized activity at any time and outside any formal program.

When researchers bring security vulnerabilities to the attention of companies and organizations, they should assume good faith until proven otherwise.

The question of whether an entity operating a program can tell the difference between a well-intended researcher and a criminal becomes philosophical or even irrelevant. Outside of the program, any criminal activity is possible and often likely. Inside the program, only good and non-criminal deeds are rewarded.

The above text describes the general case. Additionally, there can be a special case of a bug bounty program in which the program-operating entity indeed does offer special access or benefits to the participants. For instance, a company may provide test accounts or other credentials to participating researchers so that they may venture deeper into the computer system in their hunt for vulnerabilities to report and be rewarded for. In such programs, the participating researchers go through additional vetting and screening. The exact nature of the screening depends on the company's or organization's preferences and may include verification of identity and tax ID, verification of home address, criminal background check, and so on. With these additional screening requirements, the operator of the bug bounty program guards itself against malicious actors gaining access to the program in question.

For an overview of the motivations of ethical hackers and for personal profiles of a number of them, we recommend reading the 2018 Hacker Report that is available from HackerOne, Inc., on our website www.hackerone.com and by contacting us by e-mail at info@hackerone.com.

Question 2. What is the role of bug bounty programs when faced with extortion attempts?

Answer. Extortion has absolutely no role in bug bounty programs.

Whenever a situation develops that may indicate an extortion attempt, HackerOne advises the sponsor of the program (its customer) to notify and work with law enforcement for guidance and instructions. It is always the entity with the bug bounty (or vulnerability coordination) program that determines whether conduct by a hacker or hackers is authorized or unauthorized. Bug bounty platform providers such as HackerOne act as a preventative service.

There are situations where immature researchers may ask for a bounty in an impolite or even threatening way. Often, such situations can be de-escalated with the help of mediation and diplomacy. Hackers do commonly suggest or ask for specific bounty amounts from the vendor.

The size of the bounty is largely determined by the severity of the vulnerability, and severity can be properly assessed only by the customer. So the finder is in a position of no control at all over the payment outcome. To balance this, they often make suggestions, requests and claims for specific bounties in the hope that the customer will be open to suggestions. As many hackers are young and all of them are impatient, the language of such requests may not seem proper to someone not familiar with the trade, even though the hacker has the best of intentions.

Question 3. According to your testimony, the diversity and scale of the hacker community allows the "hacker-powered security" model to identify vulnerabilities that automated scanners and permanent penetration testing teams will not. Can you please further explain this sentiment? Are there any metrics or numbers that are able to cite to quantify the effectiveness of the model over other approaches?

Answer. Customers on HackerOne have resolved more than 65,000 unique security vulnerabilities to date by working with the hacker community. A good portion of these customers have reported back to HackerOne that they are finding vulnerabilities that they could not otherwise detect with scanners or penetration testing (also called pentesting). The strongest metric in support of hacker-powered security is the fact that even after deploying scanners and pentests there are innumerable security vulnerabilities that bug bounty and vulnerability disclosure programs identify.

There are a number of reasons for this. A key reason is that scanners and penetration testing are limited in scope whereas hacker-powered security is broad and diverse.

A scanner has been programmed by engineers to detect specific previously known vulnerability types, but it is limited in its ability to modify its search or "think outside the box." Though useful, scanners cannot find what humans can. Penetration tests are conducted by humans and therefore represent more intellectual variety and creativity than scanners. But they cannot measure up against a broad and creative collection of external researchers. Penetration tests follow pre-defined guide-

lines and are designed to test for a specific set of vulnerabilities. Often, customers are more eager to get a clean report than to find all possible vulnerabilities.

In both the case of scanners and of penetration testing, the customer is paying a fixed price for effort. But in the case of hacker-powered security, the customer pays for result. Hackers do not get paid unless they find something of value to the customer. This leads the hackers to try harder and think more creatively, and that in turn leads to superior results.

Question 4. Your testimony described vulnerability disclosure programs with the motto of "If you see something, say something," and further elaborates how the outside hacker will be invited to disclose the vulnerability to the system's owner. During the disclosure process, is it a common practice for the hacker to actually take exposed data in order to demonstrate proof of vulnerability to the company? If so, is there a standard type or amount of data that these [sic] is needed for the hacker to demonstrate authenticity?

Answer. The amount of evidence that it is prudent to collect when discovering a security vulnerability is a topic of great interest to the security community. On the one hand, the hacker is bound and committed by the program rules not to cause harm or obtain any data that is not needed for the work. On the other hand, there are situations where perhaps the only way of demonstrating that a breach could be possible is to actually exfiltrate some data.

Entities that operate bug bounty programs declare on their program page the rules for the hackers. Typically, they will prohibit data exfiltration, as this example from a prominent bug bounty program shows: "Findings not eligible for bounty: . . . Internal pivoting, scanning, exploiting, or exfiltrating data from internal [company name] systems."

It should be noted that a hacker may not initially know what is inside a data file found. In order to determine the nature of the file, the hacker may have to open it, which for practical purposes may mean downloading it, which amounts to exfiltration. If the contents are irrelevant, then no harm was done. If the file contains pointers to other data sources, or perhaps credentials to another system, then this is valuable information for resolving the security problem. But if the contents turn out to be customer or personal information, then the hacker must immediately erase any such copies of the file and refrain from opening it or using it again. The determination of whether it is permissible to open the file or not can be made only after the file has been opened.

Question 5. HackerOne's 2018 Hacker Report and a 2016 study conducted by the National Telecommunications and Information Administration (NTIA) both indicated that profit is a relatively limited motivation among hackers participating in coordinated vulnerability disclosure programs. Given the panel's experience with professionals in this field, could you please further describe the predominant motivators?

Answer. In the course of its business, HackerOne has enabled tens of thousands of hackers to find and help fix over 65,000 security vulnerabilities. The motivations behind the hackers' work are as diverse as the group. In the hacker surveys we have conducted, we consistently see hackers operating under multiple motivations.

Financial rewards are essential and important, but they are far from the only motivation. The presence and success of numerous vulnerability disclosure programs (*i.e.,* programs that pay no financial rewards) serve as a clear indicator that there are plenty of hackers ready to hunt for security vulnerabilities for other than pecuniary reasons. For instance, in the various programs by the Department of Defense, about 3,000 vulnerabilities have been reported into the vulnerability disclosure program and 600 within the bug bounty programs.

Many hackers hack for the intellectual challenge. They want to learn more and they are eager to know that they have the skill to find a hole in the armor of a famous company or government entity. Being thanked or acknowledged by a prestigious vulnerability disclosure program is a great motivation.

Often, hackers hack in order to find like-minded people and be able to collaborate with them. It is a reward in itself to be able to interact with someone with unusual skill or intellect.

Others hack for the pragmatic reason of advancing their careers. The list of vulnerabilities found that each hacker has on their individual HackerOne page serves as evidence of their skills. It helps them gain entry to colleges and universities or to land a security job at a company or other organization.

For many, there is an altruistic motive in hacking. They want to make the world a more secure place. They want to contribute to society. They have a sense of duty and feel that if they know how to detect vulnerabilities, it is their mandate to report them to the owners of the various systems.

Question 6. Would you agree that it is absolutely critical for companies to administer any vulnerability disclosure program responsibly based on sound principles (such as those included in DOJ's 2017 guidelines) as it has obvious impacts on industry-wide use of these types of programs that are proven to protect consumers?

Answer. Yes, HackerOne applauded the U.S. Department of Justice for its 2017 guidelines for vulnerability disclosure programs (VDP). The DoJ's guidance reflects best-practices across the industry and is a critical document for any organization. Indeed, in many ways, HackerOne is dedicated to facilitating the responsible implementation of VDPs across the broad spectrum of vulnerable entities in line with the DoJ's guidance.

Question 7. Given the unique national security aspects of working with DOD, I am interested to hear more about HackerOne's involvement in the vulnerability disclosure programs aiding our Armed Services, starting with the "Hack the Pentagon" program and followed by the "Hack the Army" and "Hack the Air Force 1.0 and 2.0."

Answer. The Department of Defense's Defense Digital Services pioneered the first ever Federal bug bounty challenge, "Hack the Pentagon," in 2016. The DoD is continuing to do so by engaging with the global hacker community through its ongoing vulnerability disclosure policy.

Since the Hack the Pentagon program launched in 2016, over 3,600 vulnerabilities have been resolved in government systems through the bug bounty and vulnerability disclosure challenges on HackerOne. Working with the ethical hacker community supplements the useful work the DoD's internal security teams are already doing.

Hack the Army

The Hack the Army Bug Bounty program ran from Wednesday, November 30, 2016 to Wednesday, December 21, 2016. Hackers reported more than 118 valid unique security issues.

Through this program, the Army was able to tap into the reservoir of diverse hackers on HackerOne, many of whom would otherwise not work with the Army, augment the work the Army red teams are already doing to help secure their systems and networks, and increase the security of mission critical systems and networks that house information critical to military recruiting.

The Army chose as its target digital assets that might have been used as a stepping stone for reaching personally identifying information about Army recruits—colloquially referred to as "the crown jewels." Ensuring this data was secure was a high priority for DoD because of the sensitivity of the information for America's potential war fighters.

The most significant vulnerability found was due to a series of chained vulnerabilities. A researcher could move from a public-facing website, *goarmy.com,* and get to an internal DoD website that requires special credentials to access. The researchers got there through an open proxy, meaning the routing was not shut down the way it should have been. The researcher, without even knowing it, was able to get to this internal network because there was a vulnerability with the proxy and with the actual system. On its own, neither vulnerability is particularly interesting. Paired together, they become critical.

Automated testing tools are not capable of such leaps of logic. It requires a highly skilled and creative researcher (or team of researchers) to chain together a number of independent flaws in order to create a path to the critical inside of the system.

The Army remediation team that owns and operates the websites, as well as the Army Cyber Protection Brigade, acted quickly. Once the report was submitted, they were able to block any further attacks, and ensure there was no way to exploit this chain of vulnerabilities.

Hack the Air Force

The Hack the Air Force Bug Bounty program ran from May 30, 2017 to June 23, 2017, with nearly 300 individual hackers participating in the bug bounty challenge. More than 50 hackers earned bounties for reporting more than 207 valid unique security vulnerabilities, the first of which was reported in less than a minute from the start of the program.

Some of the vulnerability reports received an initial response time of less than a minute by the Air Force security teams. The average time to resolution during the challenge was 4 days. What this means is that the Air Force's security team was extremely fast at processing reports, verifying them and resolving bugs, making the systems more secure faster.

Hack the Air Force 2.0

On December 9, 2017, the first day of the challenge, 24 hackers met in New York City and participated in a live hacking event—the first ever to include Federal government participation on-site. DoD and U.S. Air Force personnel worked alongside the vetted and pre-selected hackers to simultaneously report security flaws and remediate them in real-time. Together, they collaborated to find 55 of the 106 total vulnerabilities during this nine-hour hacking event.

Twenty-seven trusted hackers successfully participated in the Hack the Air Force bug bounty challenge—reporting 106 valid vulnerabilities and earning a total of $103,883. Hackers from the U.S., Canada, United Kingdom, Sweden, Netherlands, Belgium and Latvia participated in the challenge. In this event, the highest single bounty of any Federal program—$12,500—was awarded.

Question 8. More specifically, were there lessons learned from the earlier programs that your company addressed and implemented in the more recent programs?

Answer. Working with its DoD counterparts, HackerOne and the security research community continue to improve its programs. We regularly revise and improve our internal process descriptions and our external program guidelines in order to reduce the risk of failure in a program and to increase the overall productivity and effectiveness of hacker-powered security. We also continually learn more about the digital assets of our customers so that we can provide better advice on which assets to include in a program, and at what phase of the program.

As our customers develop a thorough expertise in operating a bug bounty program, we may recommend events where hackers and the security team of the customer are brought together for a live hacking event. We did so during "Hack the Air Force 2.0" and the results exceeded expectations.

Hack the Air Force targeted operationally significant websites and online services. The goal of the program was to explore new approaches to its security, and to adopt the best practices used by the most successful and secure software companies in the world. The preliminary results indicate nearly doubling the results of the first Hack the Pentagon program a year earlier.

With every DoD bug bounty the pool of invited participants has grown, with the intent of opening it wider to continue to include all qualified participants. By now, every person on HackerOne is legally permitted to participate in the DoD's vulnerability disclosure program (VDP). To date, the DoD's VDP has resolved more than 3,000 security vulnerabilities.

Question 9. How did your company account for the specific capabilities and functions of the different services your company worked with?

Answer. The key to success in a bug bounty or vulnerability disclosure program lies in diversity of approach and specificity of skill among the hackers. That is why HackerOne has established the world's largest community of security researchers, also known as white hat hackers. By having an enormous pool to draw from, we ensure that for each particular program there is a large enough group of hackers with the particular skills needed. We record and keep track of skill profiles in our hacker database. When a new program launches, we can find the hackers most likely to have the required skills.

As new customers launch programs on HackerOne, a useful cross-pollination of skills often happens. The new customer typically brings along hackers with deep skills in their particular digital asset. These hackers can then find other programs with similar profiles. And from those other programs, existing hackers may engage in the new program. In this way, over time, individual hacker skills are strengthened, and the overall skill profiles in the HackerOne community become more complete.

Additionally, both HackerOne and its clients may arrange for additional education, training and briefing of hackers in specific areas of technology. The more information there is available, the sharper the skills and the better the results of bug bounty programs.

Arguably the best source of learning for ethical hackers is the Hacktivity feed () where vulnerability reports are being published by various companies and government agencies for others to learn from once the vulnerability has been fixed and removed.

Question 10. Please explain the utility of a combined pool of Federal employee and outside participants.

Answer. The success of cyber security is measured not by how many good events there are but by how many bad events can be avoided. The best results are achieved by multiple layers of security. Even if one layer occasionally fails, there is another layer that will catch the deviation from the norm.

Cyber security starts with the design of the digital system. This is the first layer of security. Later in the software lifecycle comes quality assurance, which also removes weaknesses. When a digital asset is ready for production use, it still needs testing and validation. This is where internal and external bug hunting teams come into the picture. Internal teams of employees have the benefit of inside knowledge of the system. External teams of hackers have the benefit of lack of bias. These and other, more technical, layers of security are needed for the best outcome.

A theme we heard over and over again while working with the DoD is that military and civilian personnel need hands-on training whenever possible. This keeps their skills sharp and allows them opportunities to see unique tactics from a highly skilled researcher community. Allowing employees to participate in bug bounty programs provides realistic training experiences in a controlled environment, at a low cost.

Question 11. Your testimony states that $250,000 is the current maximum bounty listed across all programs that the company administers for its clients. Are the maximum bounty amounts pre-determined in agreements with your client companies?

Answer. On HackerOne's platform, it is the customer that sets the bounty criteria, often based on a recommendation from HackerOne. HackerOne maintains a set of recommended bounty amounts that we derive from historical bounty payment data, adjusting for size and ambition level of the program in question. The bounty amount is typically a function of the severity of the vulnerability and the value of the digital asset in which the vulnerability was found.

The client company has the full right to deviate from their own criteria and pay out higher bounties than advertised. As a matter of fact, many programs do not publish or advertise any maximum bounty.

In addition to bounties, customers can choose to pay individual bonuses to hackers. For instance, if a hacker has prepared an unusually well-researched and well-written vulnerability report to the customer, the entity may choose to reward the hacker with a bonus on top of the bounty. The bonus amounts are typically small. In 2017, less than 5 percent of all hacker rewards were bonuses.

Question 12. Your testimony stated that the Computer Fraud and Abuse Act is in need of modernization to prevent liability of hackers acting in good faith in identifying vulnerabilities to protect consumers. Do you have any specific recommendations related to modernizing the law?

Answer. Current law, particularly the Computer Fraud and Abuse Act (CFAA), does a disservice to the Internet and its citizens. Congress should amend it to reflect the modern-day needs of the country's cybersecurity community, including the value and necessity of voluntary disclosure programs.

The CFAA fails to define the terms "without authorization" or "exceeding authorized access," which are key elements of the law. This broad undefined language has resulted in the CFAA being called one of the most controversial, confusing, and inconsistently interpreted laws in the country. We suggest that the law should clarify "without authorization" and distinguish between bad intent on the one hand, and good intent or innocent lack of intent on the other.

While intended as a criminal law preventing malicious hacking, a 1994 amendment to the bill allows for civil actions. We suggest that the CFAA focus on criminal liability rather than civil liability. Much of the chilling effect created by the law originates from its broad interpretation in civil cases, where the burden of proof is reduced.

HackerOne also suggests that violations of contractual obligations, such as a website's terms of service, must not form a basis for criminal charges. Further, it should be clarified in the law that if access to data is already authorized, gaining that access in a novel or automated way is not a crime (*i.e.,* changing IP addresses, MAC addresses, or browser User Agent headers). Finally, minor violations of the CFAA should be punishable with minor penalties, ensuring the punishment fits the violation.

HackerOne urges Congress to modernize the CFAA and related laws to reflect the necessity to fight cybercrime with modern-day tools and processes, including particularly voluntary disclosure programs.

Response to Written Questions Submitted by Hon. Brian Schatz to Marten G. Mickos

Question 1. I have been working to make the process of software vulnerability disclosures more transparent and accountable. As part of this effort, Senators Gardner, Johnson, Klobuchar, and I introduced the PATCH Act. Do you support the PATCH Act?

Answer. We believe in the general and overarching principles of finding, fixing and disclosing security vulnerabilities. We as a e society should make every effort to detect security vulnerabilities and have them corrected by the owner of the system before the vulnerability can be exploited by criminals or other adversaries. Once the responsible owner of a system has remediated the vulnerability, or after a reasonable time of being advised of the existence of a vulnerability, it is in society's best interest to make this information publicly known. In our increasingly connected world, it is rare that critical lessons learned from a vulnerability are limited to a single organization. We also acknowledge that the government from time to time will have valid and specific reasons of a national security character not to report or disclose a known security vulnerability. Such withholding of vulnerability information from the owner of the system in question should be allowed temporarily only when required to address a specific and significant nation security threat. To the degree the PATCH Act validates and enforces these principles, we support the act.

Question 2. HackerOne's code of conduct clearly forbids extortion or blackmail. Yet, after the 2016 incident, Uber still remains a client of HackerOne and is listed on its platform. Was Uber's payoff to its extortionists not a violation of HackerOne's code of conduct? Was their account suspended or penalized in any manner?

Answer. Based on our observations and investigations, Uber is not and has not been in violation of HackerOne's terms and conditions or code of conduct for customers. HackerOne did not suspend or penalize Uber's customer account in any manner.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO KATIE MOUSSOURIS

Question. If we are going to increase the size and expertise of our cybersecurity workforce it is essential that we commit to expanding educational opportunities for American students. That's why I introduced the bipartisan Innovate America Act with Senator John Hoeven. Provisions from this bill became law as part of the Every Student Succeeds Act. They will improve students' access to STEM education by allowing states to award funding to create or enhance a STEM-focused specialty school or a STEM program within a school. Minnesota has received $4 million of these grants and will be making awards soon.

Ms. Moussouris, how significant is the current skills gap in the cybersecurity workforce?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO KATIE MOUSSOURIS

Question 1. There are serious questions about the disclosure timeline and process of the "Spectre" and "Meltdown" flaws. Do you believe that the right entities were involved in the research and disclosure process leading up to public notification? How could this be improved?

Answer. *No Response Provided.*

Question 2. What should be the threshold for disclosing vulnerabilities to the U.S. government? As the cyber threat model evolves, how and when should this threshold change?

Answer. *No Response Provided.*

Question 3. I have been working to make the process of software vulnerability disclosures more transparent and accountable. As part of this effort, Senators Gardner, Johnson, Klobuchar, and I introduced the PATCH Act. Do you support the PATCH Act?

Answer. *No Response Provided.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO JUSTIN BROOKMAN

Question 1. I introduced the Seniors Fraud Prevention Act with Senator Susan Collins, the Chair of the Senate Committee on Aging, to help the Federal Trade Commission (FTC) more effectively combat senior fraud. When personal information has been compromised online, identity theft and other fraud can follow consumers for years. My bill would help fight scams designed to strip seniors of their assets by helping educate seniors about fraud schemes and improving monitoring and re-

sponse to fraud complaints. This bill was passed by the Commerce Committee last year and I am happy to say it passed the Senate in August.

Mr. Brookman, what additional resources or authority at the FTC would be helpful in protecting consumers' personal information?

Answer. There are a number of important steps that I believe Congress should undertake to improve the FTC's ability to protect consumer privacy. These include:

- *Enact statutory privacy protections.* The United States is outlier in that it is one of the few nations that does not provide legal protections for most personal data. Instead, only a few isolated pockets of information (such as medical history, data about children, and video rental records) are protected—and even some of those protections are being rolled back.[1] In lieu of dedicated privacy authority, the Federal Trade Commission has leveraged existing consumer protection law to challenge some privacy violations, but its legal authority is extremely constrained. Most of the FTC's privacy cases have been brought under its *deception* authority, meaning that the FTC can only act if a company proactively deceives a consumer about its data practices. Absent affirmative transparency and choice obligations, many companies evade this liability by offering only vague and inscrutable information about its practices in privacy policies that consumers rarely read. The FTC has more recently brought privacy cases under its *unfairness* authority, but such cases require a showing of "substantial injury"—and what constitutes a substantial privacy injury is a legal uncertainty.[2] Congress could dramatically improve privacy protections and consumers' rights by enacting privacy legislation modeled on the Fair Information Practice Principles;[3] Consumers Union would be more than happy to collaborate with your office and other interested members of Congress in crafting what such legislation would look like.
- *Statutory penalties for lawbreaking.* The Federal Trade Commission lacks the legal authority to obtain civil penalties in the considerable majority of its cases—instead, it can only obtain injunctive relief and offer restitution to injured consumers (though again, restitution is challenging in the privacy realm where injuries are difficult to quantify). As such, companies are able to treat legal challenges merely as a cost of doing business. The FTC should be able to obtain reasonable civil penalties in order to sufficiently deter wrongdoing, both for violations of a new privacy statute as well as its existing Section 5 legal authority.
- *Ability to issue clarifying regulations.* Unlike many regulatory agencies, the Federal Trade Commission generally lacks the ability to issue regulations under the Administrative Procedure Act. This limitation prohibits the agency from issuing more precise guidance to companies and consumers as to what behavior is prohibited, relying instead on establishing legal norms through litigation and negotiated consent decrees. We urge Congress to provide the FTC with this authority, both for a new privacy statute as well as for Section 5.
- *Staffing.* The Federal Trade Commission needs more resources to perform its consumer protection mission. Despite the U.S. economy more than doubling in size since 1980, the size of the FTC staff has—to say the least—failed to keep up. Moreover, other agencies are increasingly pushing their own responsibilities to the FTC, especially on privacy—from the Federal Communications Commission[4] to the National Highway Traffic and Safety Administration.[5] Further, some FTC critics have called upon the FTC to litigate more its cases—instead of relying upon settlement agreements—in order to create binding and reliable rules (though, as noted above, this could also be accomplished through rule-

---

[1] *See, e.g.,* Kimberly Kindy, *How Congress dismantled Federal Internet privacy rules,* WASHINGTON POST, May 30, 2017, *https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html?utm_term=.11a7cf766dad.*

[2] The Federal Trade Commission recently hosted a public workshop on this topic. *See Informational Injury Workshop,* FEDERAL TRADE COMMISSION, Dec. 12, 2017, *https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.*

[3] Bob Gellman, *Fair Information Practice Principles: A Basic History,* Apr. 10, 2017, *https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.*

[4] Amir Nasr, *Trump's Repeal of Internet Privacy Rules Shifts Regulatory Powers to FTC,* MORNING CONSULT, Apr. 7, 2017, *https://morningconsult.com/2017/04/04/trumps-repeal-internet-privacy-rules-shifts-regulatory-powers-ftc/.*

[5] Joe Jerome, *NHTSA Automated Vehicles Guidance Punts Privacy to the FTC and Congress,* CENTER FOR DEOMCRACY & TECHNOLOGY, Sep. 22, 2017, *https://cdt.org/blog/nhtsa-automated-vehicles-guidance-punts-privacy-to-the-ftc-and-congress/.*

making).[6] However litigating against more well-resourced companies is labor intensive, and the Commission will need considerably more attorneys in place to pursue such as a strategy. In addition to additional legal support, I strongly support funding more technical staff at the FTC in order to competently police online privacy and related issues, both within substantive divisions such as the Division of Privacy and Identity Protection, but also in the Office of Technology Research and Investigation (or OTECH) which supports the entire Consumer Protection Bureau mission.

Question 2. During your time at the FTC, did you notice any trends in how new technology was being used to exploit seniors?

Answer. In my experience, the Federal Trade Commission takes very seriously its obligation to protect all citizens, but especially segments of the population that may be vulnerable to particular practices. Through its Every Community Initiative, the FTC has tried to identify various ways that predators are more likely to target certain populations.[7] A recent FTC Fraud Report found that while senior citizens were not more likely to be targeted with fraud generally, they were more likely to be targeted by certain scams, such as fraudulent prize promotions, timeshare fraud, and fraudulent medical claims.[8] Tech support scams was another such category, where attackers try to exploit unfamiliarity with technology to sign consumers up for unneeded, high-cost technical assistance—or worse, hold a consumer's computer hostage until a ransom has been paid.[9] The FTC has brought a number of tech support scam enforcement actions,[10] and in 2016 held a public workshop on the growing menace of ransomware.[11] Robocalls are another common—and growing—frustration of older Americans, and the FTC along with the FCC have taken a variety of actions to try to combat their rise.[12] Consumers Union has also advocated a number of additional steps that policymakers should take, including requiring phone companies to offer to all consumers comprehensive tools to block spoofed and unwanted calls, at no charge, and without delay.[13]

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BRIAN SCHATZ TO JUSTIN BROOKMAN

Question 1. There are serious questions about the disclosure timeline and process of the "Spectre" and "Meltdown" flaws. Do you believe that the right entities were involved in the research and disclosure process leading up to public notification? How could this be improved?

Answer. Given the unprecedented scope of the Spectre and Meltdown vulnerabilities and my lack of practical experience in incident response, I am hesitant to severely criticize the disclosure timing and processes that were used. Multi-party coordination can be extraordinarily challenging under less complicated circumstances, and there are inevitable and difficult trade-offs between the values of concealing information to prevent leaks that could harm consumers with sharing information to the diverse parties who will have to address the vulnerabilities. I question the assessment that the vulnerabilities were not being actively exploited, and how it was used as a rationale for not sharing information with US–CERT. Further, I believe that several companies' initial public statements understating the scope of the problem was counterproductive. It is my hope that the companies involved will undertake a rigorous assessment of what worked well and what did not in order to learn

---

[6] Tom Struble, *Reforming the Federal Trade Commission Through Better Process,* R STREET, Dec. 2017, *http://2o9ub0417chl2lg6m43em6psi2i.wpengine.netdna-cdn.com/wp-content/uploads/2017/12/122.pdf.*

[7] *Every Community,* FEDERAL TRADE COMMISSION, *https://www.consumer.ftc.gov/features/every-community.*

[8] Testimony of Lois Greisman before the Senate Special Committee on Aging, *Stopping Senior Scams: Developments in Financial Fraud Affecting Seniors,* Feb. 15, 2017, *https://www.ftc.gov/system/files/documents/public_statements/1069573/p134405_commission_testimony_re_stopping_senior_scams_senate_02152017.pdf.*

[9] *Id.*

[10] *E.g.,* Press Release, *FTC Obtains Settlements from Operators of Tech Support Scams,* FEDERAL TRADE COMMISSION, Oct. 26, 2017, *https://www.ftc.gov/news-events/press-releases/2017/10/ftc-obtains-settlements-operators-tech-support-s cams.*

[11] *Fall Technology Series: Ransomware,* FEDERAL TRADE COMMISSION, Sep. 7, 2016, *https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware.*

[12] *Robocalls,* FEDERAL TRADE COMMISSION, *https://www.consumer.ftc.gov/features/feature-0025-robocalls.*

[13] *E.g.,* Maureen Mahoney, *Letter from Consumers Union to Senators Bill Nelson et. al,* Apr. 5, 2018, *g/wp-content/uploads/2018/04/CU–CFA-Robocalls-S.-134.pdf.*

from this experience, as this will certainly not be the last major vulnerability that threatens devices and services across the ecosystem.

While the Spectre/Meltdown incident may provide valuable lessons about incident response and coordination, I believe there are potentially more important lessons about how security often receives insufficient attention during product design. The current legal framework does not provide strong enough incentives for companies to safeguard against these types of vulnerabilities in the first place. Functions such as speculative execution prioritize performance at all costs without sufficient weighting of the risks of exploitation. Unfortunately, companies do not bear the full costs of security vulnerabilities, as it is consumers who end up bearing the burdens of identity theft, impaired functionality, and the need to replace products. While companies who experience a security breach may face the loss of consumer goodwill, in a vulnerability as fundamental as Spectre and Meltdown, consumers may not even know which company to blame, given that so many products and system layers were affected. In concentrated industries with only a handful of providers (or fewer), the insufficiency of after-the-fact market pressure is an even greater problem.

Consumers often feel helpless in the wake of incidents such as these, unsure of which products are vulnerable, and if so, to what types of attacks. While there are some useful guidelines for consumers to keep in mind (keep software updated, use tracker blockers to stop unnecessary interactions with third-party servers), consumers are usually not in the best position to ensure security on their systems. Companies should have legal obligations to deploy and maintain reasonable security measures, proportionate to the risks borne by both by the companies and others. In some cases, this may compromise performance, if the security risks outweigh the performance loss. However, in many cases, this can be remediated through addressing other prevalent anti-consumer inefficiencies, such as device bloatware and excessive reliance on third party tracking code.

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.