

BIG DATA: PRIVACY RISKS AND NEEDED REFORM IN THE PUBLIC AND PRIVATE SECTORS

HEARING BEFORE THE COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES ONE HUNDRED SEVENTEENTH CONGRESS SECOND SESSION

FEBRUARY 16, 2022

Printed for the use of the Committee on House Administration



Available on the Internet:
<http://www.govinfo.gov/committee/house-administration>

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON HOUSE ADMINISTRATION

ZOE LOFGREN, California, *Chairperson*

JAMIE RASKIN, Maryland

G. K. BUTTERFIELD, North Carolina

PETE AGUILAR, California

MARY GAY SCANLON, Pennsylvania

TERESA LEGER FERNÁNDEZ, New Mexico

RODNEY DAVIS, Illinois,

Ranking Member

BARRY LOUDERMILK, Georgia

BRYAN STEIL, Wisconsin

CONTENTS

FEBRUARY 16, 2022

	Page
Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors	1
OPENING STATEMENTS	
Hon. Zoe Lofgren, Chairperson	1
Prepared statement of Chairperson Lofgren	4
Hon. Rodney Davis, Ranking Member	6
Prepared statement of Mr. Davis	8
WITNESSES	
Hon. Hugh N. Halpern, Director, Government Publishing Office	10
Prepared statement of Hon. Halpern	13
Shoshana Zuboff, Charles Edward Wilson Professor Emerita, Harvard Business School	33
Prepared statement of Prof. Zuboff	35
Caitriona Fitzgerald, Deputy Director, Electronic Privacy Information Center	53
Prepared statement of Ms. Fitzgerald	55
Marshall Erwin, Chief Security Officer, Mozilla Corporation	74
Prepared statement of Mr. Erwin	76
Daniel Castro, Vice President, Information Technology and Innovation Foundation	82
Prepared statement of Mr. Castro	84
QUESTIONS FOR THE RECORD	
Hon. Hugh N. Halpern, Director, Government Publishing Office, responses	110
Caitriona Fitzgerald, Deputy Director, Electronic Privacy Information Center, responses	114
Marshall Erwin, Chief Security Officer, Mozilla Corporation, responses	119
Daniel Castro, Vice President, Information Technology and Innovation Foundation, responses	121
SUBMISSIONS FOR THE RECORD	
February 25, 2022, National Association of Assistant United States Attorneys, submission	126
June 22, 2021, Ranking Member Davis letter to Chairperson Lofgren, submission	128
February 15, 2022, CATO letter to Chairperson Lofgren and Ranking Member Davis, submission	130
United States District Court for the District of Columbia, <i>United States v. Michael A. Sussmann</i> , submission	137
Singman, Brooke, Fox News, <i>Clinton campaign paid to 'infiltrate' Trump Tower, White House servers to link Trump to Russia, Durham finds</i> , submission	150

BIG DATA: PRIVACY RISKS AND NEEDED REFORMS IN THE PUBLIC AND PRIVATE SECTORS

WEDNESDAY, FEBRUARY 16, 2022

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The Committee met, pursuant to call, at 2:03 p.m., via Webex, Hon. Zoe Lofgren [Chairperson of the Committee] presiding.

Present: Representatives Lofgren, Raskin, Aguilar, Scanlon, Leger Fernández, Davis, Loudermilk, and Steil.

Staff Present: Sean Jones, Legislative Clerk; Jamie Fleet, Staff Director; Eddie Flaherty, Chief Clerk; Khalil Abboud, Deputy Staff Director; Tim Monahan, Republican Staff Director; Caleb Hays, Republican General Counsel and Deputy Staff Director; Nick Crocker, Republican Deputy Staff Director; Gineen Bresso, Republican Special Counsel.

The CHAIRPERSON. So the Committee on House Administration will come to order.

I note that a quorum is present. As we begin, I would note that we are holding this hearing in compliance with the regulations for Remote Committee Proceedings pursuant to House Resolution 8.

Generally, we ask Committee Members and witnesses to keep their microphones muted when not speaking to limit background noise, and all of us will need to unmute ourselves when seeking recognition or when recognized to speak. Witnesses will also need to unmute themselves when recognized for their testimony or when answering a question.

Members and witnesses, the rules require that we keep our cameras on at all times. Even if you need to step away for a moment, please do not leave the meeting or turn your camera off. I would also like to remind Members that the regulations governing remote proceedings require that Members cannot participate in more than one committee proceeding at the same time.

At this time, I ask unanimous consent that all Members have five legislative days in which to revise and extend their remarks and have any written statements be made part of the record.

And, hearing no objections, that is ordered.

I also ask unanimous consent that the chair be authorized to declare a recess of the Committee at any point.

And, without objection, that is also so ordered.

We are here today to confront one of the central challenges of our digital age. As nearly every facet of our society and economy has moved online, ever greater amounts of digital data are collected about each of us, spanning everything from who we are, to what

we like, to who we are—who we communicate with, to what we do, often in minute detail.

While this mass data collection has some productive and valuable applications, it comes with profound risks that we are only beginning to truly understand, let alone to regulate effectively.

Privacy, as it is conventionally understood, means control over one's own personal information and the freedom to decide what to share, with whom, and how. We are all familiar with the classic privacy harms, whether it is government surveillance, identity theft and other economic crimes, or the social and economic harm that can befall us when some intimate details of our life become public against our will.

All these risks are still very much at play today with the rise of the internet and data-centric business models of many online firms. However, in some ways, privacy has become a catchall term for a larger and even more profound set of potential risks, some of which are truly novel or at least fundamentally different in the digital age.

What does it mean for our basic autonomy as individuals when both the government and private companies can amass large profiles about each of us and use them to predict and even potentially manipulate our behavior? What does it mean for our economy when some of the most popular online products and services revolve around opaque data collection and personalization? And what does it mean for our democracy when these data practices shape the public discourse and the flow of news and information? And what does it mean that, as individuals and internet users, we have little or no meaningful ability or visibility into how any of this really works, let alone genuine control over it?

The American public has long been deeply concerned about these questions. For example, in 2020, the Pew Research Center found that half of Americans had limited specific online activities out of privacy fears. The same year, another poll found that 88 percent are frustrated that they don't have more control over their personal information online.

I will note that these fears kind of cross many divisions in our society: economic, racial, geographic, and partisan. For all these reasons, the time for a comprehensive Federal policy framework is long overdue. There have been many proposals and lots of talk, but little or no action or clear progress.

I will note that Representatives Anna Eshoo and I have introduced the Online Privacy Act in several Congresses, including this one. This legislation sets forth the most thorough and aggressive set of privacy rights among the major proposals with the clearest restrictions on a wide variety of abusive and troubling data practices, and the strongest mechanisms to enforce the law and make digital privacy rights more than just an abstraction.

The Online Privacy Act also contains a set of privacy obligations on Legislative Branch agencies that this Committee oversees, requiring the Government Publishing Office, the Library of Congress, the Smithsonian, and the Chief Administrative Officer of the House to each identify concrete privacy risks in their operations and to take appropriate remedial steps.

Many of the risks and policy questions around data cut across both public and private sectors. We can take lessons from both in determining the best ways to address them. I am hopeful that today's hearing will not only advance this conversation, but also reinvigorate congressional attention on digital privacy toward the ultimate enactment of major reforms.

With that, I am now pleased to recognize our Ranking Member, Congressman Rodney Davis, for any comments that he would like to make.

Welcome, Rodney.

[The statement of The Chairperson follows:]

**ZOE LOFGREN, CALIFORNIA
CHAIRPERSON**

JAMIE RASKIN, MARYLAND
G.K. BUTTERFIELD, NORTH CAROLINA
PETE AGUILAR, CALIFORNIA
MARY GAY SCANLON, PENNSYLVANIA
VICE CHAIRPERSON
TERESA LEGER FERNANDEZ, NEW MEXICO

JAMIE FLEET
STAFF DIRECTOR

One Hundred Seventeenth
Congress of the United States
House of Representatives

COMMITTEE ON HOUSE ADMINISTRATION

1309 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6157
202-225-2061 | CHA.HOUSE.GOV

**RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER**

BARRY LOUDERMILK, GEORGIA
BRYAN STEIL, WISCONSIN

TIM MONAHAN
MINORITY STAFF DIRECTOR

Chairperson Zoe Lofgren

February 16, 2022

**Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors
Opening Statement**

We are here today to confront one of the central challenges of our digital age. As nearly every facet of our society and economy has moved online, ever greater amounts of digital data are collected about each of us, spanning everything from who we are, to what we like, to who we are, who we communicate and to what we do often in minute detail.

While this mass data collection has some productive and valuable applications, it comes with profound risks that we are only beginning to truly understand, let alone to regulate effectively. Privacy, as it is conventionally understood, means control over one's own personal information and the freedom to decide what to share, with whom, and how. We are all familiar with the classic privacy harms, whether it is government surveillance, identity theft and other economic crimes, or the social and economic harm that can befall us when some intimate details of our life become public against our will.

All of these risks are still very much at play today with the rise of the Internet and data-centric business models of many online firms. However, in some ways, privacy has become a catchall term for a larger and even more profound set of potential risks, some of which are truly novel or at least fundamentally different in the digital age.

What does it mean for our basic autonomy as individuals when both the government and private companies can amass large profiles about each of us and use them to predict and even potentially manipulate our behavior? What does it mean for our economy when some of the most popular online products and services revolve around opaque data collection and personalization? And what does it mean for our democracy when these data practices shape the public discourse and the flow of news and information? And what does it mean that, as individuals and internet users, we have little or no meaningful ability or visibility into how any of this really works, let alone guide genuine control over it?

The American public has long been deeply concerned about these questions. For example, in 2020, the Pew Research Center found that half of Americans had limited specific online activities out of privacy fears. The same year, another poll

found that 88 percent are frustrated that they don't have more control over their personal information online. And I will note that these fears kind of cross many divisions in our society: economic, racial, geographic, and partisan. For all these reasons, the time for a comprehensive Federal policy framework is long overdue. There have been many proposals and lots of talk, but little or no action or clear progress.

I will note that Representatives Anna Eshoo and I have introduced the Online Privacy Act in several Congresses, including this one. This legislation sets forth the most thorough and aggressive set of privacy rights among the major proposals with the clearest restrictions on a wide variety of abusive and troubling data practices, and the strongest mechanisms to enforce the law and make digital privacy rights more than just an abstraction.

The Online Privacy Act also contains a set of privacy obligations on Legislative Branch agencies that this Committee oversees, requiring the Government Publishing Office, the Library of Congress, the Smithsonian, and the Chief Administrative Officer of the House to each identify concrete privacy risks in their operations and to take appropriate remedial steps.

Many of the risks and policy questions around data cut across both public and private sectors. We can take lessons from both in determining the best ways to address them. And I am hopeful that today's hearing will not only advance this conversation, but also reinvigorate congressional attention on digital privacy toward the ultimate enactment of major reforms.

Mr. DAVIS. Well, thank you, Madam Chairperson.

And thanks to our witnesses for joining us for today's hearing. It is a hearing on a rare topic for this Committee, but no doubt an important one: online data privacy. Yet policy discussions on creating nationwide privacy standards and a framework for enforcement need to take place in the primary committees of jurisdiction: Energy and Commerce and the Judiciary. It is clear to me that this discussion should be led by those primary committees and jurisdiction, and we should let them work out the underlying policy details before we consider application to the Legislative Branch.

304 bills have been referred to this Committee by the House, yet we are devoting our time today to this topic. It is rare we are even meeting on potential legislation this Congress. We have had exactly one other hearing on the policy underlying a bill and exactly zero markups.

Further, this Committee has not held comprehensive standard oversight hearings with our entities in nearly three years. For us not even to discuss FEC or EAC oversight hearings in an election year is shocking to me.

Eight months ago, I sent a letter to the Chairperson asking for this Committee to fulfill its duty and conduct oversight hearings with each of our Legislative Branch entities. Eight months later, I still have not received a response from the Chairperson, and the Committee continues to shirk its duties.

I look forward to this Committee having more oversight hearings soon to address the concerns that fall more directly within this Committee's jurisdiction.

Regarding the topic at issue today, the call for a workable national framework, increased transparency, and overall accountability in the technology industry, is all but universal at this point. Data privacy is at the forefront because it affects everyone. We all see the need. As a parent of three young adults, I believe this issue deserves not only Congress' attention, but it also demands it.

All anyone has to do is watch the news to see how data privacy affects everyone. Last week, filings by Special Counsel John Durham alleged that, in 2016, Democratic operatives, perhaps including Marc Elias, who multiple members of this Committee are familiar with, in his attempts to—in his attempts to challenge the legitimacy of elections, sought to exploit their access to non-public and/or proprietary internet data to create a narrative tying President Trump to Russia, in the words of one outlet, to infiltrate Trump Tower and White House servers to link Trump to Russia. Talk about an election subversion. Unbelievable.

So, a responsible and workable nationwide solution for data privacy that can protect Americans' privacy and also curb bad political actors from attempting to subvert our political discourse is necessary. I know that our Chairperson has a special interest in this topic, and I imagine that her desire to raise the profile of her legislation is why we are here today. So, let's discuss it.

I spoke with my good friend, Energy and Commerce Ranking Member Cathy McMorris Rodgers, since her committee would be primary, and she offered me a lot of good thoughts, things I assume she would say if this hearing were before her committee, where it belongs first.

First, we share more personal information online now than ever before. As the internet has grown, so has the opportunity for our personal information to be used by people or businesses that we never intended.

Second, privacy does not end at State lines. This is a nationwide Commerce Clause issue that requires a congressional response. Americans cannot rely on conflicting State laws to keep their information safe. A patchwork solution is not viable for a concern that affects all of us. The only way to provide transparency in how Americans' information is collected, used, and shared is with a uniform approach.

We must also ensure that any congressional response is forward thinking and comprehensive while still being workable for compliance. Solutions that do not account for burdens placed on small businesses and innovators, such as the GDPR in the EU or the CCPA in California, are doomed to fail.

Finally, those who misuse personal information must be held accountable. There have been proposals that call for the creation of a new Federal agency to enforce its provisions. The Federal Trade Commission already has jurisdiction over these matters, as well as a longstanding relationship with the States' AGs. Creating a new agency to do the FTC's job is bureaucratic waste at the highest level.

Americans' call for a comprehensive solution to Big Data privacy issues is loud and clear, and they deserve an answer, an answer that is built with bipartisan buy-in, transparency, and accountability.

Even though this Committee isn't where we should be hosting this portion of this discussion, I am looking forward to today's panels, and I yield back.

[The statement of Mr. Davis follows:]

ZOE LOFGREN, CALIFORNIA
CHAIRPERSON

JAMIE RASKIN, MARYLAND
 G.K. BUTTERFIELD, NORTH CAROLINA
 PETE AGUILAR, CALIFORNIA
 MARY GAY SCANLON, PENNSYLVANIA
VICE CHAIRPERSON
 TERESA LEGER FERNANDEZ, NEW MEXICO

JAMIE FLEET
 STAFF DIRECTOR

One Hundred Seventeenth
Congress of the United States
 House of Representatives

COMMITTEE ON HOUSE ADMINISTRATION

1309 LONGWORTH HOUSE OFFICE BUILDING
 WASHINGTON, DC 20515-6157
 202-225-2061 | CHA.HOUSE.GOV

RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER

BARRY LOUDERMILK, GEORGIA
 BRYAN STEIL, WISCONSIN

TIM MONAHAN
 MINORITY STAFF DIRECTOR

Ranking Member Rodney Davis

February 16, 2022

Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors
Opening Statement

Thank you, Madam Chairperson. And thanks to our witnesses for joining us for today's hearing. It is a hearing on a rare topic for this Committee, but no doubt an important one: online data privacy. Yet policy discussions on creating nationwide privacy standards and a framework for enforcement need to take place in the primary committees of jurisdiction: Energy and Commerce and the Judiciary. It is clear to me that this discussion should be led by those primary committees of jurisdiction and we should let them work out the underlying policy details before we consider application to the Legislative Branch.

304 bills have been referred to this Committee by the House, yet we are devoting our time today to this topic. And it is rare we are even meeting on potential legislation this Congress. We have had exactly one other hearing on the policy underlying a bill and exactly zero markups. Further, this Committee has not held comprehensive standard oversight hearings with our entities in nearly three years. For us not even to have a discussion about FEC or EAC oversight hearings in an election year is shocking to me.

Eight months ago, I sent a letter to the chair asking for this Committee to fulfill its duty and conduct oversight hearings with each of our Legislative Branch entities. Eight months later, I still have not received a response from the chair, and the Committee continues to shirk its duties.

I look forward to this Committee having more oversight hearings soon to address the concerns that fall more directly within this Committee's jurisdiction. Regarding the topic at issue today, the call for a workable national framework, increased transparency, and overall accountability in the technology industry, is all but universal at this point. Data privacy is at the forefront because it affects everyone. We all see the need. And, as a parent of three young adults, I believe this issue deserves not only Congress' attention, it demands it.

All anyone has to do is watch the news to see how data privacy affects everyone. Last week, filings by Special Counsel John Durham alleged that, in 2016, Democratic operatives, perhaps including Marc Elias, who multiple Members of this

Committee are familiar with, in his attempts to challenges the legitimacy of elections, sought to exploit their access to non-public and/or proprietary Internet data to create a narrative tying President Trump to Russia, in the words of one outlet, to infiltrate Trump Tower and White House servers to link Trump to Russia. Talk about an election subversion. Unbelievable.

So a responsible and workable nationwide solution for data privacy that can protect Americans' privacy and also curb bad political actors from attempting to subvert our political discourse is necessary. I know that our chair has a special interest in this topic, and I imagine that her desire to raise the profile of her legislation is why we are here today. So let's discuss it. I spoke with my good friend, E&C ranking Member Cathy McMorris Rodgers, since her committee would be primary, and she offered me a lot of good thoughts, things I assume she would say if this hearing were before her committee, where it belongs first.

First, we share more personal information online now than ever before. As the Internet has grown, so has the opportunity our personal information to be used by people or businesses that we never intended. Second, privacy does not end at States lines. This is a nationwide Commerce Clause issue that requires a Congressional response. Americans cannot rely on conflicting State laws to keep their information safe. A patchwork solution is not viable for a concern that affects all of us. The only way to provide transparency in how Americans' information is collected, used, and shared is with a uniform approach.

We must also ensure that any congressional response is forward thinking and comprehensive while still being workable for compliance. Solutions that do not account for burdens placed on small businesses and innovators, such as the GDPR in the EU or the CCPA in California, are doomed to fail. Finally, those who misuse personal information must be held accountable. There have been proposals that call for the creation of a new Federal agency to enforce its provisions. The Federal Trade Commission already has jurisdiction over these matters, as well as a longstanding relationship with the States' AGs. Creating a new agency to do the FTC's job is bureaucratic waste at the highest level.

Americans' call for a comprehensive solution to Big Data privacy issues is loud and clear, and they deserve an answer, an answer that is built with bipartisan buy-in, transparency, and accountability. Even though this Committee isn't where we should be hosting this portion of this discussion, I am actually looking forward to today's panels, and I yield back the balance of my time. Thank you, Madam Chairperson.

The CHAIRPERSON. The gentleman yields back.

I just would note for the record that the Committee's jurisdiction is generally determined by House Rules specifically, House Rule X—and this Committee has been, along with other committees, assigned jurisdiction.

I want to thank the Ranking Member for his comments.

I would also like to recognize our first witness, who is someone who has led the U.S. Government Publishing Office with great distinction of late.

He is the 28th person to lead the GPO since it opened its doors in 1861 and has served in this role in 2019. Hugh Nathaniel Halpern was selected this month—the GPO was selected as one of the best employers in the country, ranking first on Forbes' list of midsize agencies in government services.

I really do think, Hugh, that it is a reflection on your leadership as well as your fine staff at the GPO.

As you know—this is not your first time to be a witness—your entire written statement will be made part of the record, and we would ask that you summarize your testimony in about five minutes.

So, Mr. Halpern, you are now recognized for five minutes.

STATEMENT OF HUGH HALPERN, DIRECTOR, GOVERNMENT PUBLISHING OFFICE, WASHINGTON, D.C.

Mr. HALPERN. Thank you so much and thank you for acknowledging the achievement of making that Forbes list. I will take some credit if it is assigned, but it really belongs to the men and women here at GPO. So, thank you so much for having me today, both to the Chairperson and to the Ranking Member, and all the Members of the Committee.

I appreciate the opportunity to testify about GPO's approach to handling personally identifiable information, commonly known as PII. On behalf of GPO's more than 1,500 craftspeople and professionals, know that we take our responsibility seriously to protect PII every day.

GPO operates as a hybrid. It is a government agency that operates as a business, complete with customers, products, and profit and loss. Thus, we face many of the same kinds of problems facing private-sector firms when it comes to the handling of PII.

GPO is entrusted with PII belonging to our teammates, customers, and, by nature of our business, the general public. Robust protection of PII is critical to building trust with our customers and stakeholders. Without that trust, we can never achieve our vision of an America informed.

GPO operates a Privacy Program overseen by our privacy officer in our information technology business unit. This program establishes a framework for the protection of PII itself, regardless of how it is stored, as well as the protection of related information systems.

The program has several fundamental principles. First, access to PII is limited to only those agency teammates and contractors with a specific need.

Second, each business unit has someone who is responsible for the privacy function and answers to that business unit's leadership.

Third, any GPO teammate or contractor that suspects a breach in PII security is obligated to report the problem as soon as possible.

Fourth, violations will be addressed by appropriate corrective action, including termination for our teammates, debarment for contractors, and criminal prosecution if appropriate.

While my written testimony goes into more detail as to how this program works, today I would like to talk about three separate examples of privacy issues at GPO and how we deal with them.

First, GPO and its print procurement contractors produce materials that require the use of PII. For instance, GPO's Security and Intelligent Documents Unit manufactures and personalizes trusted traveler smart cards, such as the global entry card used to at border crossings for identification and for expedited processing.

By the very nature of these products, GPO must handle vast amounts of highly sensitive PII within our systems. GPO works closely with its customers to maintain a series of firewalls that ensure that GPO only receives encrypted PII that is only decrypted when it is needed to produce and distribute those cards. When GPO finishes production of the product, that PII is scrubbed from our systems. You can't leak information you don't have.

Second, there are vast amounts of PII included in some of our regular publications, such as the Congressional Record and Federal Register. The good news, particularly with the Federal Register, is that most of that PII is contained in historic volumes, and very little is being published currently. Where it is, we have both automated and manual systems to redact that information from our digital collections when we find it.

The bigger challenge is with historic information, particularly as we work to digitize older collections. For instance, at one time, it was common for the Department of Defense to include military officers' Social Security numbers on promotion lists later printed in the Congressional Record.

As we digitize volumes that contained that information, we scan for it and redact that PII in preparation before posting it on Govinfo.gov, our ISO-certified, trusted digital repository. And, while we alert our partners when we find PII in tangible collections that we don't possess ourselves, we do not have the resources to visit every collection across the country and manually redact that information.

The third and final category are instances where the information is not quite PII but is information that people don't want easily accessible on the internet. This comes up most often with our collection of U.S. court opinions on Govinfo.gov, and that is the repository's single largest collection of data. It is understandable that some parties of Federal court cases may not want that information to be easily accessible, and they often come to GPO asking us to remove that opinion from our collection.

However, it is important to remember that GPO is only making that data accessible, and it is not our data. Our Library Services Division refers individuals to petition the owner of the data, the Administrative Office of the U.S. Courts, to have the opinion sealed and removed from our systems if the judge determines that public disclosure is problematic.

I hope that this overview of our operations was helpful in your exploration of this critical issue. I look forward to answering any questions you may have and assisting the Committee with its inquiry.

Thank you so much.

[The statement of Mr. Halpern follows:]



THE HONORABLE HUGH NATHANIAL HALPERN
Director
United States Government Publishing Office

**Testimony of Government Publishing Office
Director Hugh N. Halpern before the
Committee on House Administration Hearing on
“*Big Data: Privacy Risks and Needed Reforms in the
Public and Private Sectors*”**

February 16, 2022
2:00 P.M.

U.S. GOVERNMENT PUBLISHING OFFICE

732 North Capitol Street, NW | Washington, DC 20401-0001
www.gpo.gov | facebook.com/usgpo | twitter.com/usgpo | instagram.com/usgpo



Thank you Chairperson Lofgren and Ranking Member Davis for inviting me to testify today on behalf of the more than 1,500 craftspeople and professionals who make up the Government Publishing Office to discuss our approach to the critically important issue of protecting personally identifiable information (PII) and safeguarding individual privacy. GPO is entrusted with PII belonging to our teammates, customers, and, by nature of our business, the general public. We devote considerable time, attention, and resources to securing and protecting that information, and we are always interested to share our experiences and learn from the experience of others.

Robust protection of PII is critical to building trust with our customers and stakeholders. Without that trust, we can never achieve our vision of an *America Informed*.

GPO's Approach to PII Protection

GPO's approach to protecting PII is laid out in our Privacy Program, which is overseen by our Privacy Officer, who reports to our Chief Information Officer. The Privacy Program establishes a framework for the protection of PII from unauthorized use, access, disclosure, or sharing as well as the protection of related information systems from unauthorized access, modification, disruption, or destruction.

Originally established in 2010, the Privacy Program was most recently updated in 2021 through GPO Directive 825.41B. GPO's privacy program applies to our teammates and contractors alike. It rests on a few fundamental principles:

- First, the only people who may access PII held by GPO are authorized Agency staff and contractors trained in the protocols required to protect that information;
- Second, each business unit within GPO must have a designated privacy point of contact that reports directly to the business unit leadership;
- Third, it is the affirmative obligation of any GPO employee or contractor who suspects a breach of PII security to promptly report the concern; and
- Fourth and finally, the directive provides that failure to comply with agency PII protection standards and procedures is grounds for corrective actions up to and including termination for employees, debarment for contractors, or even criminal prosecution if appropriate.

As part of his duties in administering the Privacy Program, GPO's Privacy Officer coordinates two significant processes—GPO's ongoing PII management and protection and responding appropriately to a possible PII security breach.

GPO's Privacy Officer proactively requires the periodic performance of Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA) by GPO business units. These assessments evaluate how those business units maintain, secure, and utilize PII in their daily operations.

The second process relates to how GPO responds to a potential breach of systems containing PII, and is referred to as the Privacy Incident Response Team (PIRT) Framework. Whenever a GPO employee or contractor suspects a breach in PII security has occurred that individual is required to report it through a Privacy Incident Report shared with his or her supervisor. The Business Unit Manager and Privacy Point of Contact are then responsible for notifying GPO's Privacy Officer, who convenes the Privacy Incident Response Team to assess the scope of the breach and determine the scope of the Agency's response, up to and including the possibility of alerting the United States Computer Emergency Readiness Team (US-CERT) within the Department of Homeland Security.



In developing and executing these policies and procedures that guide its Privacy Program, GPO has sought to follow the recommendations laid out by the National Institute of Standards and Technology (NIST) in their "Guide to Protecting the Confidentiality of Personally Identifiable Information (Special Publication 800-22)," which identifies six imperatives for Federal agencies:

- Identifying all the PII residing in their environment;
- Minimizing the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission;
- Categorizing PII by confidentiality impact level;
- Applying the appropriate safeguards for PII based on the confidentiality impact levels;
- Developing an incident response plan to handle breaches involving PII; and
- Encouraging close coordination among their chief privacy officers, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII.

I believe GPO's Privacy Program is responsive to each of them, and today I want to highlight two of them that have particular salience to GPO's administration of its **govinfo** trusted digital repository and GPO's overall system of providing online access to Government information. Those recommendations relate to the categorization of PII by confidentiality impact levels and the application of safeguards based on those confidentiality impact levels.

Changes in technology have driven everyone's concern about the ease with which personal information is available. On the one hand, there is a lower concern about a stray piece of PII in a printed document in a library because it is comparatively more difficult to access. Similarly, using that information in a nefarious way is also more difficult without our modern technology infrastructure. On the other, because we have made this information more accessible, the threat from the use of that information has also exponentially increased.

For example, in preparation for this hearing one of my colleagues remarked how as late as the 1990s his college used students' social security numbers as identifiers on their student ID cards, something that was completely unremarkable at the time. Another colleague remarked how a relative found her social security number because it appeared on a digitized Department of Defense document. Things that were at one time innocent practices with little impact are today serious breaches of protocol with potential wide-ranging impacts.

For GPO this amounts to a dual challenge — keeping current with the most effective strategies to protect PII in our current operations while also devising flexible solutions to PII disclosure challenges caused by the fact sensitive PII simply wasn't protected during the initial publication of tens of thousands of Government publications already in circulation.

To do this effectively without compromising the American people's access to important Government information, GPO differentiates among the various types of PII potentially housed in the collections that we either provide access to or host.

Using the NIST report and related OMB guidance to inform our approach to PII categorization, GPO considered the potential harm of disclosure to determine which forms of PII should be considered high-impact PII versus those that should be categorized as low-impact PII.



By differentiating between these two categories of PII, GPO believes it improves its ability to restrict or suppress that identifying information which is most likely to cause specific individuals harm upon disclosure without compromising the utility of the underlying public documents. GPO's definition of high-impact PII includes personal identification numbers issued by government or financial institutions printed in conjunction with an individual's name, such as full or partial social security numbers, taxpayer identification numbers, patient identification numbers, financial account numbers, or credit card numbers. In our view the unauthorized disclosure of these types of information are likely to pose the greatest risk to any individual.

Low-impact PII in our view would include a person's name, their street address, phone number, names of family members, and photographic images. Attempting to redact every such instance in which low-impact PII could be found in Government publications we believe would present a far greater challenge, with less obvious benefit, and considerably greater impact on the usability of the affected publications.

Protecting PII in GPO's Daily Operations

GPO's operations consist of two basic activities: producing Government information and identification documents and making Government information widely available. The Agency needs to protect any PII in both of those modes.

On the production side, there is no better example than what we do with PII than our work on secure identification documents. GPO's Security and Intelligent Documents operations involve significant amounts of PII and we take extraordinary steps to protect it every day. The PII data that comes into GPO is encrypted and once it is in our servers it is then decrypted and sent to the production machines. For instance, GPO manufactures and personalizes several varieties of identification cards. Specifically, the trusted traveler "smart" cards are used at both the Northern and Southern border crossings for identification and for expedited processing. By the very nature of these products, GPO must handle vast amounts of highly sensitive PII within our systems. GPO works closely with its customers and their contractors to maintain a series of firewalls that ensure that GPO only receives encrypted PII that is only decrypted when it is needed to produce and distribute those cards. When GPO finishes production of the product, that PII is scrubbed from our systems.

Much of our work to protect PII occurs as we work to make Government information more available. Since the passage of the GPO Electronic Information Access Enhancement Act of 1993, GPO has been working to broaden the availability of Government information on the Internet. What began nearly 30 years ago with the *GPO Access* website posting the daily Congressional Record and little more has now grown into the world's only ISO-certified trusted digital repository giving people worldwide free public online access to authenticated Government content. The volume of documents available online has grown to nearly 2.2 million packages, with over 320,000 packages added in FY 2021 alone. Last month we celebrated the 9 billionth retrieval of content through GPO's system of online access since the original *GPO Access* site first went live in 1994.

Today, 97 percent of all Federal Government publications are "born" digital and the growth in the electronic accessibility of Government information is significant enough that I recently established the Task Force on a Digital Federal Depository Library Program, comprised of 23 members representing the Depository Library Council, the Depository Library Community, Federal Agency partners, and library associations, to study what until recently might have been unthinkable: the feasibility and advisability of moving toward an all-digital Federal Depository Library Program.



Recognizing the importance of protecting PII that may have inadvertently found its way into our publicly accessible systems, the Superintendent of Documents adopted a policy requiring the redaction of high-impact PII whenever it is discovered within the publicly accessible files in GPO's system of online access, or within content being prepared for ingest into that system. To fulfill legal requirements of GPO's affiliate agreement with the National Archives and Records Administration, we must maintain unredacted preservation copies of those materials, but the PII can be redacted from the versions we put online.

In addition, because GPO's Partnership program provides a guide to materials that are beyond GPO's direct custodial control, GPO also takes proactive steps to alert those entities with which GPO has partnership agreements whenever GPO learns that materials in those partner's collections might reveal high-impact PII. This enables GPO's content partners to take appropriate action to redact or obscure PII that they may not have been aware existed.

In 2008, the Joint Committee on Printing authorized GPO to redact PII in the electronic access copies of congressional publications. For congressional publications published today, GPO can act immediately to suppress protected information in access copies of those publications without altering the underlying content. Where GPO's task becomes more challenging is when we are engaged in efforts to digitize historical collections of documents.

The most prominent example of this may be GPO's efforts in partnership with the Library of Congress to digitize every volume of the Congressional Record back to its inception in 1873 and make them available through **govinfo**, a project that GPO completed in 2019. The Library of Congress digitized millions of pages that contained thousands of instances of PII — particularly the entire or partial social security numbers of thousands of individuals. Many of these occurrences were related to the promotion of career staff, particularly in the Armed Forces.

While we haven't caught every single instance of PII appearing in the electronic copies of congressional publications prior to making them available to the public in electronic form, we have the infrastructure in place to systematically discover and remediate PII on an ongoing basis.

GPO maintains a contract with a vendor to provide high-impact PII redaction services that covers both historic, digitally-imaged content, as well as content already within the **govinfo** system on an as-discovered basis. Specifically, this contract covers both historic and contemporary congressional publications including the Serial Set, Digitized Hearings, the Daily Congressional Record, Bound Congressional Record, and any future digitization work that has the potential to contain PII. We also have access to software that enables us to manually redact such high-impact PII whenever we encounter it.

To date, our PII redaction contract has allowed us to find and redact 1,598 documents containing instances of PII both in publications currently found on **govinfo** as well as those we are in the process of digitizing. With significant anticipated digitization efforts planned in the future — for example the ongoing multi-year collaborative project with the Law Library of Congress to digitize the U.S. Congressional Serial Set and the possible digitization of thousands of congressionally mandated reports identified in the Congressionally Mandated Reports Act currently being considered in Congress — we expect to make considerable additional PII redaction investments in the years ahead.

Congress should be aware, however, that even if we are immensely successful in redacting such high-impact PII from those Government information collections we are digitizing ourselves, those we make available directly via **govinfo**, and those we provide access to via partnership agreements with other institutions, it is unlikely that such sensitive PII information will vanish completely from the Internet. This is because other well-intentioned institutions have undertaken efforts to make digitized copies of such Government publications electronically available in the past, and still others may choose to do so in the future.



To date, a few of the institutions who have done some of this work have demonstrated a willingness to remove high-impact PII from their digitized collections when we have made them aware of the issue, and Google Books and HathiTrust are worthy of recognition on that front. Still others lack either the resources to find and redact PII in their collections or the interest in doing so, and there's no legal authority for GPO to compel those third parties to take that action.

Additionally, it is important to remember that much of this digitization is based on existing tangible documents and those documents are distributed across the Nation, even if they aren't always easy to locate. By way of illustration, through the early 1990s GPO produced and disseminated nearly 20,000 copies of the Congressional Record each day — more than 10 times our current production level — so we are certain that there will always be some tangible copies of Government documents that contain PII that we will be unable to locate. The sheer number of tangible copies of older Government publications that contain sensitive, high-impact PII is going to continue to pose challenges for all of us for years to come.

Beyond the issue of the exposure of high-impact PII, there's the more general issue of potentially embarrassing personal information about specific individuals becoming easier to find because of the increasing electronic accessibility of Government publications. It has been my experience that people often try to conflate information which is merely unflattering with PII in order to hide that information from public view. It's important that we maintain the distinction between the two.

We can all agree that it is in the public interest to ensure that U.S. Federal Court opinions are accessible via the United States Courts Opinions (USCOURTS) collection on [govinfo](#). This is a collaborative effort between GPO and the Administrative Office of the United States Courts to provide public access to opinions from select United States appellate, district, and bankruptcy courts, consistent with the E-Government Act's requirement for the substance of all written opinions, issued after April 16, 2005, to be made available in a text searchable format [Section 205 of Pub. L. No. 107-347].

However, on occasion individuals referenced in those opinions prefer that their involvement with those proceedings remain unknown and demand that GPO remove the relevant opinion from the collection. It is critical to understand that this data belongs to our customers and GPO has no independent authority to redact or remove an opinion, and per the Superintendent's policy with regard to online redactions or removal from collections, GPO will only take action in response to a request from the originating agency, the courts that issued the opinions.

When these inquiries arise, GPO refers individuals to the Administrative Office of the U.S. Courts for information about applying to the court that issued the opinion, which may decide to seal the opinion if the judge determines it warrants withdrawal from public access.

That concludes my testimony. I hope that this discussion of our practices, procedures, and capabilities was helpful to the Committee and I welcome your questions.



Hugh Nathaniel Halpern,
GPO Director

Hugh Nathaniel Halpern is the U.S. Government Publishing Office (GPO) Director, the agency's chief executive officer. The agency is responsible for publishing and printing information for the three branches of the Federal Government. Halpern is the 28th person to lead GPO since the agency opened its doors for business on March 4, 1861, the same day Abraham Lincoln was inaugurated as the 16th President of the United States. President Donald Trump nominated Halpern to be GPO Director on October 17, 2019, and the U.S. Senate confirmed him on December 4, 2019.

Biography

Prior to coming to GPO, Halpern held a succession of leadership positions during his 30 years on Capitol Hill. He served as the Director of Floor Operations for the Speaker of the U.S. House of Representatives. In that role, Halpern was the highest-ranking floor staffer in the House and served as Speaker Paul Ryan's Chief Advisor on all procedural matters. He managed the daily floor operations of the House, served as the liaison to all leadership offices, and oversaw legislative interactions between The White House, House and Senate. In 2018, he received the John W. McCormack Award of Excellence, the highest award given to a staff member in the House. The award recognizes a lifetime of bipartisan service to the House.

In addition to his position in the Speaker's Office, Halpern has more than a decade of experience serving on the senior leadership staff. He has a proven track record of successfully leading teams to achieve results.

During his career, he served half a dozen different committees in both policy development and procedural roles. During his 11 years on the House Committee on Rules, Halpern served as Staff Director leading the management and terms of debate on the House floor. In 2001, he was named General Counsel by Chairman Mike Oxley for the newly established House Committee on Financial Services. During his tenure, the committee provided legislation addressing terrorist financing and money laundering, improving investor confidence in the wake of the Enron and WorldCom scandals and granting consumers important new tools to fight identity theft. During the 1990s, Halpern served on the House Committee on Energy and Commerce, where he handled a variety of legislative issues, including automobile safety, insurance, FTC consumer protection and tobacco regulation. Halpern began his career in Congress as an intern for Rep. E.G. "Bud" Shuster in 1987.

Halpern served a number of temporary positions during his time on Capitol Hill. He was the Parliamentarian to the First Select Committee on Homeland Security, which created the Department of Homeland Security, General Counsel to the Select Committee to investigate the voting irregularities of August 2, 2007, and Assistant Parliamentarian to the 2008, 2012, and 2016 Republican National Conventions.

A native of Hollidaysburg, PA, Halpern received bachelor's and master's degrees in Political Science from American University in 1991 and 1992, respectively. He also received a law degree from George Mason University in 1997. Halpern has been included in Roll Call's list of 50 most powerful Congressional staffers 14 times and featured in a National Journal profile as one of "The New Power Players" on Capitol Hill.



U.S. GOVERNMENT PUBLISHING OFFICE

732 North Capitol Street, NW | Washington, DC 20401-0001

www.gpo.gov | facebook.com/usgpo | twitter.com/usgpo | instagram.com/usgpo

The CHAIRPERSON. Thank you so much, Director Halpern. It is great to hear this testimony.

Now is the time when Members can ask questions, and we will turn first to the Ranking Member, Mr. Davis, for five minutes of his questions.

Mr. DAVIS. You would think I would know how to work the mute button right now, Madam Chairperson. I apologize for the delay.

Hugh, great to see you, man.

Mr. HALPERN. You, too.

Mr. DAVIS. I looked. The last time you were called to testify before this Committee was on March 30—March 3rd of 2020—

Mr. HALPERN. Yes.

Mr. DAVIS [continuing]. Nearly two full years ago. It is nice to finally have you back, but I wish it was to get a comprehensive update on GPO's operations and the initiatives you have launched and successes you have had as well as the agency's health post pandemic.

Unfortunately, we are here to talk about a much narrower topic, but one that GPO clearly excels at, and that is protecting the PII, the personally identifiable information you spoke about, and its work to print passports, create global entry cards, and other sensitive projects.

In your testimony, you shared the impressive work GPO has undertaken to follow the recommendations laid out by the National Institute of Standards and Technology and their guide to protecting the confidentiality of PII.

Do you currently believe that you, as the Director of GPO, have all the necessary authority to continue a high level of excellence in protecting PII?

Mr. HALPERN. Thanks so much for the question.

The short answer is, at the moment, I think we do. We have got the authority we need to work with our customers, to design systems that protect the PII that they give us, and in our relationship with our own vendors, whether that is a contractor that we hire on behalf of the executive branch for work that they are doing for the IRS or other government agencies. That—we are able to construct systems that protect that level of PII.

Now, one of the things that we must remain vigilant about is the PII of our own teammates. And frankly, if there was a large body of PII that the agency maintains, that is it. It is our payroll information. It is our time and attendance information. It is our personnel files.

We work both with folks here in the building and with our vendors over at the Department of Agriculture, who handle our payroll and other systems, to make sure that that information is protected. We are doing our level best to protect the nearly 1,600 people who work here at GPO from running into any problems, as well as the information of anybody who is working with GPO or working with our customers.

Mr. DAVIS. Great. How often is GPO's privacy program reassessed or updated to remain at this high level of effectiveness?

Mr. HALPERN. So, it is constantly undergoing assessment. Our—the directive that governs our privacy program is supposed to be reviewed, I believe, every three years. We are constantly going

through our policies, our procedures, and our actual practices to make sure that we are doing our level best. And that is both on the digital side, where we have an extremely competent team on our information technology team, but also just with our safety and security team.

Now, I get an update three, four times a year as our safety and security team walks the building to make sure that things are shipshape. I can tell you they have flagged folks who have inadvertently left PII sitting on their desk, not having it stored properly. So, it is a good reminder to all of us that we need to be proactive in protecting this information, whether it is digitally or tangibly here in the real world.

Mr. DAVIS. I couldn't agree more.

One last question. What has GPO learned from the OPM breach that happened several years ago?

Mr. HALPERN. I think it is very similar to the lessons that a lot of government agencies are learning. We have got to secure our systems, and we spend a lot of resources. We have a dedicated appropriation for that purpose. And it requires a lot of vigilance on our part.

And, you know, knock on wood, thank God, certainly during my tenure here, we have not had anything that even indicated that folks were close to a breach of those kinds of systems, and it is something we dedicate a lot of resources to every single day.

And, you know, the one thing that the OPM breach, I think, taught all of us is you can't rest on your laurels. Security needs to be everybody's job every single day.

Mr. DAVIS. Well, thanks, Hugh.

Thank you, Madam Chairperson. I yield back.

The CHAIRPERSON. Thank you.

I now recognize Mr. Raskin for his questions for five minutes.

Mr. RASKIN. Thank you, Madam Chairperson, and thanks for calling this important hearing.

Ms. Fitzgerald, discrete bits of personal information can seem relatively harmless or trivial, but, when they are all combined together with other data, they can have a far more sweeping impact and create special dangers.

What lessons does this point contain for privacy regulation? What are the biggest risks that Congress should be considering in terms of the large-scale aggregation of data?

The CHAIRPERSON. I would note that Ms. Fitzgerald is on our second panel, so—

Mr. RASKIN. Oh, I am sorry. I thought I saw her there. Forgive me. Then I will come, then, to Mr. Halpern.

So, what are the greatest privacy risks that GPO faces in its operations? What are the specific harms in this area that you are most focused on right now?

Mr. HALPERN. Well, as I was saying, I think the largest single trove that we maintain over a long—over a longer period is our employees' own data. And that is something that we are focused very, very closely on protecting.

Most of the other places where we have PII and we need to focus on that, we have developed systems to make sure that we are holding onto that PII for the minimum amount of time possible.

So, for instance, in the example I used with the global entry card, we literally have a contractor sitting on the other side of the wall from our smart card manufacturing facility who will send the encrypted data that we will need to produce those cards into the smart card room, we will utilize that information to produce those cards, and then scrub that from our systems, send it back to the customer once we are done with it, so that we are not holding on to any more data than we need.

Our biggest problem in terms of other folks' data is historical data. And, as we fulfill, I think, the greater public good of working backwards and trying to digitize old records, we are going to find more PII because, frankly, twenty or thirty years ago, folks were a lot less conscious about what they were putting in a congressional hearing or the Congressional Record or the Federal Register. Because those were all tangible documents, it was a lot harder for somebody to get that information and then to do something with it, because the internet just wasn't developed as it is now.

We have got a program in place to scan for PII in those older documents. And, as we digitize them, we are working to redact that from our digital collections.

Mr. RASKIN. Thank you for that. I know that GPO routinely publishes documents and information that originate elsewhere in the Federal Government, so you are not the original custodian and source of all the information you publish. And so how does this affect your privacy policies and practices?

Mr. HALPERN. We are often the middle person in this transaction. The good example is the one I gave in my testimony about U.S. courts—court opinions. As you can well imagine, there are a lot of opinions that folks may not be happy are out there in the world or easily searchable. And, while as a general matter, that serves a greater public good, there is that problem with, you know, maybe having an opinion where there is information in there that somebody is uncomfortable with having out in the public.

So, what we have done is we have a number of different places. If you go to gpo.gov/privacy, it talks about our entire privacy program, including who you need to talk to over at the Administrative Office of the U.S. Courts to deal with a court document that may have issues.

Similarly, just a few years ago, we revamped our Ask GPO system, which is now powered by a modern contact management system. And there, we have also got links so that, if folks find an opinion or something like that that raises an issue, they can ask about it, we can root that to the proper person and make sure they get the information to talk to the Administrative Office of the U.S. Courts to get that particular record sealed if that is appropriate.

In terms of—

Mr. RASKIN. Thank you so much.

I yield back, Madam Chairperson.

Mr. HALPERN. Thanks.

The CHAIRPERSON. Thanks so much, and I will recognize the gentleman from Georgia now for his questions for five minutes, Mr. Loudermilk.

Mr. LOUDERMILK. Well, thank you, Madam Chairperson.

And, Hugh, it is good to see you again.

Mr. HALPERN. Likewise.

Mr. LOUDERMILK. I appreciate all the work that you are doing over at GPO. And you said something a few minutes ago that was music to my ears, and I have been saying this ever since I have been in Congress. It is a lesson I learned working in intelligence on the IT side when I was in the Air Force. One of the primary principles that was just engraved into our every policy we have is you don't have to secure what you don't have. If you don't need it, then discard it.

We had procedures built around that to analyze data, whether we needed it or not. You had to justify keeping it. And then it was destroyed.

The problem we have—I have been saying this ever since I have been in Congress, and especially on Financial Services Committee, as we are dealing with these same issues—is there is many in Congress and in the Federal Government that aren't applying that principle, and so much legislation is being passed that is getting the Federal Government to grab more data or forcing businesses to acquire more data of individuals, and somebody is keeping that and storing it as data that does not need to be kept.

I appreciate hearing you say that because there is very few government officials or, quite frankly, people in Congress that you ever hear say that: If you don't need it then don't keep it.

So, has GPO experienced any data breaches or identified attempted attacks in recent years?

Mr. HALPERN. So yes, on the attack side. No on the breach side. The good news is my IT security folks were doing their job, and to the best of our knowledge, we have not had a breach, certainly during my tenure or even in the years leading up to it.

Shortly after I became the Director of GPO—I still remember it—I was at an event on Saturday night at my synagogue when I suddenly learned that somebody that we believe affiliated with the Iranians had defaced the front of one of our sites. The good news is that is all the farther they got. We were able to restore that site. We are in the process—we are in the process of moving that over to a more secure infrastructure.

And, the good news is that my team has a really good process in place to make sure that our systems are secure. As updates come out, they are tested thoroughly before we do those upgrades. So we don't necessarily have—we don't necessarily have the exposures you might have from unknown vulnerabilities. So we really work hard to try and get that right.

Mr. LOUDERMILK. Well, it sounds like you are doing a good job at that, because, if you would have answered my question then, "Well, we haven't had any data breaches and no attempted attacks," I would have said, "Then you are not doing your job," because I guarantee you, you are being attacked. And, if you don't know it, then there is something wrong.

Also, the updates, they are crucial. That is what caused the Equifax data breach, was simply a failure in the IT department to not do a firmware update that was needed to be done.

So, I am comfortable with the answers you have given. And that is why we haven't seen any data breaches. In the thirty years I spent in IT and data security, I could tell you the question isn't if

you are going to be hacked; it is when. It is going to happen at some point, and it is a race to stay just ahead of the bad guy.

I use the analogy of when I used to hunt in Alaska, and we would go bear hunting. Somebody inevitably would put on a pair of tennis shoes and say: What that is for? So, well, if we see a grizzly, I want to have my tennis shoes on.

They say: Well, you can't outrun a grizzly.

They would say: No, I just have to outrun you.

All right? So, it is the same thing, is you have got to stay ahead of the bad guy and stay one step above someone else because, if they can't get into you, they will go on to somebody else.

So, it sounds like I have already heard the answer to this question, but do you have all the tools you need to keep carrying out this level of privacy and security, or is there additional things that we can do in Congress to help?

Mr. HALPERN. At the moment, I think we are in pretty good shape. The things are—we have the flexibility. We have the tools that we need. Obviously, it is always a question of resources, but, as we start automating processes here at GPO, we are really focused on figuring out how we make our dollars go farther. And that has really been one of the hallmarks of GPO all through history.

So, we are putting that emphasis on security and trying to do it with tools we have got. And, where we don't have tools, we make the investments we need. That is—you know, to some extent, that is one of our advantages. Only about twelve percent of our total revenue comes from appropriations. The rest is what we charge our customers.

So, the State Department expects us to keep their passports fully secure, and we spend a lot of money doing that. But the State Department reimburses us for those investments. And the same with our other customers. We are pretty comfortable with where we are, but we are always happy to talk about things and figure out how we can do better.

Mr. LOUDERMILK. Well, this is an ever-changing environment, and it is a job that is never done, because once you think that you are secure and you are not staying on top of it, the bad guys are going to beat us. Thank you for all you are doing.

Madam Chairperson, I yield back.

The CHAIRPERSON. The gentleman yields back.

Mr. Aguilar is recognized for five minutes.

Mr. AGUILAR. Thank you, Madam Chairperson.

And thanks, Director Halpern, for the update and the information. A lot to review here, and I appreciate your commitment to safeguarding that PII.

What I was kind of interested in is—and you talked about some of the digital versus the historical documents that you are in charge to protect. Your testimony kind of speaks to that and said that 97 percent of the Federal documents now are born digital.

So, what distinctions does GPO make between the digital versus paper documents in terms of privacy risks and how they can be addressed by your team and by the contractors, and how has that transition been to the Digital Age and the privacy risks that are associated with that on your operational side?

Mr. HALPERN. Thanks so much, sir, for that.

The short answer is that, for new documents that we produce, we have an airtight system for trying to scan those documents as we are producing them, looking for PII. As I mentioned, with the Federal Register, they are under the OPM policies regarding PII, so there is not a lot that is coming in.

We do need to check the Congressional Record, and we work very hard to redact any PII that might appear there. But I think even Congress is being more circumspect about that stuff going forward.

Our biggest problem is stuff that exists in the tangible form, so a printed paper that was printed historically twenty or thirty years ago, or even a lot longer. And what we are running into are two issues there. One is, as we are trying to digitize that information. We are taking committee hearings from the 1970s or the 1980s and trying to digitize those and put them on Govinfo.gov.

There, both our contractor and our library team are looking at those documents. Where they see and where they catch PII, we are redacting that from the digital copies that go online.

When it comes to those paper documents, we simply don't have the capacity to literally travel the world to find every copy of the Congressional Record from the late 1800s forward, check those volumes for PII, and redact them. So we are, in some respects, reliant on our partners, the Federal depository libraries and our other libraries across the world, where a lot of this information goes.

But, that said, as I mentioned before, I think, because that information is comparatively hard to access—you need to go to a physical place, and you need to open a physical volume to find that—because it is harder to access, that is a little bit lower of a threat than what is going out in the digital domain.

It is not a zero threat, but—and, where we find PII, we try to try and redact it. We just don't have the resources in terms of people, money, and all those kinds of things to do a full scrub for every place where one of these paper documents might exist in the world.

Mr. AGUILAR. Understood. And how do you kind of keep—what is the digital, you know, kind of hygiene? How do you stay ahead of the evolving threats and the digital privacy landscape piece of it? Is it through the OPM guidance? Is it through, you know, contractors, or how do you kind of stay ahead of the risks that are in front of you?

Mr. HALPERN. So, one of the great things about being a legislative branch agency is we can take the best practices all across the government. We are not necessarily confined by what OPM provides.

I know that our IT security team both works with the other CISOs here in the Legislative Branch as well as broader across the government. As we do work for our other Federal customers, we are obviously talking to them, figuring out what their requirements are, and how we can meet those. So, there is a lot of variety of avenues for us to be exposed to the sort of changing landscape and what folks' requirements are, and we are always going to make sure that our systems are designed in such a way as to protect the security of those documents.

Whether it is producing smart cards, whether it is the U.S. passport, one of the reasons that they come to GPO is because we can produce those documents securely in government facilities with the

highest quality you are going to find any place in the world and do it at a reasonable price and in a reasonable timeframe.

So——

Mr. AGUILAR. Thanks.

Mr. HALPERN [continuing]. We think we have got some advantages there.

Mr. AGUILAR. Thank you so much. Appreciate it.

I yield back, Madam Chairperson.

The CHAIRPERSON. Thank you. Mr. Steil is now recognized for five minutes.

Mr. STEIL. Thank you very much, Madam Chairperson.

Mr. Halpern, appreciate you being here today.

Long day on Zoom staring at screens for all of us, and I think we are all looking forward to getting back in person before too long. But I appreciate you being here, and I think maybe in a future Committee hearing, we will get an opportunity to talk to some of your Legislative Branch colleagues, what is just a critical issue.

I can't tell you how often I hear from folks across Wisconsin about the importance of data privacy. They are thinking about it. They are thinking about being hacked. There is really a timely Politico article that came out just a little bit ago talking about our reporters being hacked through apps. It is nonstop that this is something that we are talking about, and I think important that we are talking about it here.

The proposed piece of legislation that would mandate GPO action in the data privacy space, the Online Privacy Act of 2021 that we are talking about, were you consulted in the drafting of the legislation, specifically Section 5?

Mr. HALPERN. We were not consulted on the front end, although we did have subsequent discussions with the Committee. From our reading, it is a flexible standard in the proposed legislation, and it is something that we think we can meet with the program that we are running today, and it will give us an opportunity to take a look at and make sure that there is—if there are any places where we need to tighten things up, we definitely can do that.

Mr. STEIL. Understood. Appreciate your commentary on that. That is helpful.

Under national data privacy laws, there is really—it is really kind of a balance in ways to minimize compliance costs for small businesses while still providing appropriate levels of protection to individuals. Can you kind of comment on how you try to strike that balance?

Mr. HALPERN. So, for most of our interactions with small businesses, that is through our print procurement program. And the requirements there are largely driven by our customers.

Now, that said, there are any number of small and medium size businesses that can participate in our print production or print procurement program. To give you an idea, I was just up in Pennsylvania—I think it was a few months ago—and we visited with one of our contractors that does a lot of work with GPO. And we use that contractor specifically because they have a great system for keeping track of information and keeping track of documents with sensitive information in it and give us a great paper trail. They do a fantastic job of handling those types of jobs for us and doing it

in a way where we are confident that that information is safe and secure.

I think there are some other companies across the country that can do that work for us. There aren't a ton, to be a hundred percent honest with you. And, when we have run into problems where, say, one contractor has experienced labor shortages, which isn't something that is uncommon these days, there aren't a lot of other places to go. But some of the small and medium size businesses that we work with have gotten really good at having internal systems that can protect that information. And, frankly, sometimes they do a better job of it than some of our larger contractors.

Mr. STEIL. Great. I appreciate that feedback, Mr. Halpern.

Madam Chairperson, I will yield back.

The CHAIRPERSON. The gentleman yields back.

Ms. Scanlon is recognized for five minutes.

Ms. SCANLON. Thank you, Madam Chairperson.

Mr. Halpern, what remedial measures do the GPO have in place if one of its publications contains nonpublic personal information about a private individual, especially if it is sensitive or otherwise potentially harmful in nature?

Mr. HALPERN. Absolutely. As I mentioned, we have both automated and manual systems to redact information that is found in our digital collection.

So, for instance, let's just say for the sake of argument something slipped through tonight's edition of the Congressional Record. There was something that had some PII in it and all our checks failed. The good news is, when that is brought to our attention, our team can go in, change the record in Govinfo.gov, our trusted digital repository, and redact that information out of the digital record.

We can't really fix the printed copies, but the volume of those copies for something, say, like the Congressional Record is much smaller than it was even a decade and a half ago.

So, to give you an idea, in the 1990s, the daily circulation of the Congressional Record was north of 20,000 copies a day. Today, we are only producing about 1,500 copies a day. So, it is a much smaller universe in the printed world, and we have tools in place to fix any problems that might occur on the back end through our digital systems.

Ms. SCANLON. I mean, when you were talking about the court systems, that kind of caught my attention, because that is where I spent my pre-congressional career, and certainly judges will talk about a lot of facts as they are ruling on a case. So, you know, would an affected individual have the right or the ability to get personally identifiable information deleted, redacted, or otherwise remediated?

Mr. HALPERN. So, the way that works right now, it is not our process; it is the court's process. So, they can petition the Administrative Office of the U.S. Courts, and it is up to the judge to decide whether or not to seal those particular records or parts of a record.

And, depending on that decision, we will either pull the record out of Govinfo.gov, or put in a redacted version depending on what the constraints are of the judge's order.

As I mentioned in my testimony, this is sort of that gray area. It doesn't necessarily fall into the category of the standard PII, people's Social Security numbers, their other key identifiers. But it may describe facts that somebody is uncomfortable with. And, in those kinds of cases, we are not going to be the best folks to make a decision as to whether that needs to stay in the public domain or it needs to be removed. The judge who was involved in that case or another judge really needs to be the person who makes that decision. And, depending on what that decision is, we will act accordingly.

Ms. SCANLON. Well, if it was something within your domain, is there currently a right of an individual to be able to get personally identifiable information redacted? If, for example, a Social Security number or a—I don't know—a credit card number or something somehow had slipped through, is there a right to have it removed?

Mr. HALPERN. I can get back to you on what the statutory background is on that. I can tell you, for GPO's policies and directives, if we come across that information and can redact it from our—primarily from our digital collection, we are going to do so. And, if somebody brings that to our attention, it may not be the person whose information that is. It could be a third party.

But, if we become aware of that and we—you know, we agree that that is PII, we will make the effort to redact that from the digital side.

Ms. SCANLON. Okay. Thank you.

Madam Chairperson, I yield back.

The CHAIRPERSON. Thank you.

I now recognize the gentlelady from New Mexico for five minutes.

Ms. LEGER FERNÁNDEZ. Thank you so very much, Chairperson Lofgren. And thank you for holding this hearing, because I can tell you that this issue comes up a lot as I talk to my constituents. They are concerned, and we are concerned with regards to the manner in which our data is protected.

Director Halpern, I truly appreciated your comments about how protection of our personal data held by the government is linked to people's trust in our government, and I think you would agree that this link will only grow stronger as more of our lives move into the digital space.

I also appreciated your comments about how GPO and other Federal agencies are discussing best practices with each other. Do you believe that—can you elaborate a bit more on what we are doing here at the Legislative Branch that we might strengthen based on the information you are hearing and sharing with the other Federal agencies so that we can make sure that we have those protections against the cyber-attacks, as well as protecting individuals' personal information as you described it?

Mr. HALPERN. Sure. I will do my best.

Then—it happens on a number of different axes is probably the best way to think of it. As I mentioned before, our computer information security folks have a lot of back and forth, and there is a lot of discussion about what are those best practices, how do we secure our systems?

And, frankly, particularly with GPO and the Congress, there is a lot of interchange that occurs on a daily basis. You are sending

us information. We are sending it back to you. And we are working with the Library to make things available via Congress.gov.

So, there is a lot of discussion about those particular flows, and, frankly, what our CISOs are experiencing day to day: Where are these attacks coming from? How do you secure against them? And what are the appropriate countermeasures?

The other area that we are working on is our obligation as an employer. So, I just got the update this morning. Right now, we are at 1,547 people working directly for GPO, plus, you know, a few hundred contractors. We have an obligation to secure that information—payroll information, health information, all sorts of things.

The Chief Administrative Officer of the House has a similar obligation. So our officials are talking all the time about how we—how we maintain our systems both from the cyber standpoint and from the more mundane operational standpoint.

And as I mentioned before, my safety and security team literally walk our building. We have a million square feet under roof, and we walk every inch of that building. And one of the things that they look for is, is there PII not being stored properly?

That is a little bit harder to do in the congressional space. You know, I spent thirty years working in the House, so it is a little bit different there. But, some of those same practices, whether it is the Chief Administrative Officer or the Secretary of the Senate or House Sergeant at Arms, all of us are talking all the time to try and figure out what is the best way forward? And there is a lot of information sharing that goes on.

Ms. LEGER FERNÁNDEZ. Thank you so much. And I take it that you have no control over, you know, the fact that—and I think we will hear testimony that every search is saved and mined, right? So, as individuals might be searching within the Congressional Record for information, that—tell me, do we—do you have any way of protecting any of those searches, or is that something that is left to the individual with regards to his or her computer use and privacy settings?

Mr. HALPERN. So, it is a great question, and I will get you a more detailed answer as to the information we retain and don't retain.

The short answer is, is we try to retain the minimum amount of information we possibly can about searches in Govinfo.gov or any of our other systems.

So, for instance, in the case of Govinfo.gov, we use the smallest, most mundane kinds of cookies we possibly can. We don't track people across the internet. And, frankly, unlike Congress.gov, we don't have logins, we don't persistently save those searches for folks.

That said—

Ms. LEGER FERNÁNDEZ. I see my time has expired. I do thank you and your organization for respecting, as is proper, the privacy of the users in the documents and in the searches.

I yield back, Madam Chairperson.

The CHAIRPERSON. Thank you.

Just a couple of further questions.

First, Director Halpern, I just want to commend you and your staff for your proactive work protecting privacy. It is admirable.

And in your statement, you said you can't, if you don't save the material, it can't be abused.

And that is the principle of the Online Privacy Act, to really prevent the unnecessary retention of information, because if you don't have it, you can't data mine it, you can't abuse it.

And that is what you are doing in your agency and something that I think we want to look at. Because if you are using a search engine to search something in the Congressional Record, the search engine retains it, even though you don't.

And so, government—you are doing the right thing, but people's searches or inquiries can still be abused and manipulated.

Just two quick questions.

First, really you are doing everything with NIST and OMB guidance and your directives. You are doing that because you want to do the right thing. But it is not—your policies are not required by law at this time, are they?

Mr. HALPERN. No. The short answer is, it is one of the blessings and curses of being in the Legislative Branch.

I actually, am a big Article I guy, so I like the flexibility that this gives us to survey the landscape and pick the policies that meet our values.

Our values are we are going to protect our customer. We are going to be transparent with folks. And we are going to do everything we do, whether it is with our folks here in the building or our customers, in a respectful way. And part of being respectful is protecting that data.

The good news is, while there may not be pure statutory requirements that say you have to do this, one, we believe that our oversight committees expect us to do this, and it is the right thing to expect. And two, our customers expect us to do it.

And both of those are driving imperatives for us here at GPO, and it helps us get into the position where it is easier for us to do the right thing that we were planning to do anyway.

The CHAIRPERSON. All right.

Just one final question. In your written testimony, you mention that GPO distinguishes between high impact and low impact personally identifiable information. I am interested in how or whether you reevaluate the level of risk for different types of PII that may change over time.

And as you classify that, do you consider the potential impact when information is aggregated by third parties in combination with other personally identifiable information, for example, using machine learning or other data processing techniques that are outside of your agency?

Mr. HALPERN. We are always trying to learn. And there are a lot of very clever folks across the country who are coming up with new ways to use that sort of ubiquitous data that is out there. But we do draw a distinction between certain kinds of PIIs.

So, for instance, those unique identifiers, your Social Security number, the card numbers, or passport numbers that the Department of State or Department of Homeland Security use, those are key pieces of information that have the potential to unlock so much else, including biometrics and a whole slew of other things. We are going to work much harder to protect that information.

Lower impact data are things like addresses, photos, names, and that stuff is really kind of ubiquitous. So, for instance, when you do a special order and you are congratulating the coach of your high school football team, you are going to call that person by that name, and that is PII. But we are not going to redact that from the Congressional Record, because that, one, isn't a huge security risk, and two, if we did, it totally eviscerates the point of that special order.

The CHAIRPERSON. Exactly.

I want to thank you, Director Halpern, for your great testimony today. And as you know from your years here on the Hill, we do keep the record open if we have additional questions. So, if that occurs, we will send them right on to you and I know you will get back to us.

I just want to thank you for being here with us today. It has been very informative. And please let your team know how much we think of them and how proud we are of them.

Mr. HALPERN. Thank you very much, ma'am. I really appreciate it.

The CHAIRPERSON. Thank you.

We will now go to our second panel of witnesses and let me briefly introduce them.

First, we have Shoshana Zuboff, who is the Charles Edward Wilson Professor Emerita at Harvard Business School.

Professor Zuboff is an internationally recognized expert and the author of several major works on digital privacy issues, such as "In the Age of the Smart Machine: The Future of Work and Power" and "The Support Economy: Why Corporations Are Failing Individuals and the Next Episode of Capitalism."

Her most recent book, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power," investigates the new surveillance economy, which is driven by consumer data.

Our next witness is Caitriona Fitzgerald, who is the Deputy Director at the Electronic Privacy Information Center, or EPIC. She leads EPIC's policy work, working to advance strong privacy, open government, and algorithmic fairness and accountability laws. She recently authored, "Grading on a Curve: Privacy Legislation in the 116th Congress," which sets out the key elements of modern privacy law, including the creation of a U.S. data protection agency.

The next witness is Marshall Erwin, who is the Chief Security Officer of Mozilla, where he focuses on data security, privacy, and surveillance.

He has previously worked as a counterterrorism and cybersecurity analyst and has served as the counterterrorism and intelligence adviser to Senator Susan Collins on the Senate Homeland Security and Government Affairs Committee and was the intelligence specialist at the Congressional Research Service.

And finally, we have Daniel Castro, Vice President of the Information Technology and Innovation Foundation, or ITIF, and the Director of the Center for Data Innovation, an ITIF-affiliated research institute focusing on the intersection of data technology and public policy.

I will remind the witnesses that your entire written statements—which, by the way, are excellent—will be included and made part of our permanent record, and that that record will remain open for at least five days for additional material to be submitted.

We ask that you summarize your testimony in five minutes so that the Members of the Committee will have time to pose questions to you.

So, first, Professor Zuboff, we would love to hear from you for five minutes.

STATEMENTS OF MS. SHOSHANA ZUBOFF, CHARLES EDWARD WILSON PROFESSOR EMERITA, HARVARD BUSINESS SCHOOL; MS. CAITRIONA FITZGERALD, DEPUTY DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; MR. MARSHALL ERWIN, CHIEF SECURITY OFFICER, MOZILLA CORPORATION; AND MR. DANIEL CASTRO, VICE PRESIDENT, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

STATEMENT OF SHOSHANA ZUBOFF

Ms. ZUBOFF. Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you so much for this opportunity to discuss the challenges of privacy, privacy law, in a world without privacy.

I have spent the last 43 years of my life studying the rise of the digital as an economic force that is driving our transformation into an information civilization. Over these last two decades, I have observed as the fledgling internet companies morphed into a sweeping surveillance-based economic order founded on the premise that privacy must fall, empowered by economic operations that I have called surveillance capitalism.

Surveillance capitalism maintains core elements of traditional capitalism—private property, commodification, market exchange, growth, and profit—but these cannot be realized without the technologies and social relations of surveillance.

Hidden methods of observation secretly extract human experience, until recently considered private, and translate it into behavioral data. These methods operate outside of human awareness, engineered to do so, robbing actors of the right to know and with it the right to combat.

Ill-gotten human data are then immediately claimed as corporate property, private property, available for aggregation, computation, prediction, targeting, modification, and sales.

The theory of surveillance capitalism challenges this property claim and redefines it as theft. Surveillance capitalism was invented at Google during the financial emergency of the dot-com bust. It migrated to Facebook, became the default model of the tech sector, and is now reordering diverse industries, from insurance, retail, banking, and finance, to agriculture, automobiles, education, healthcare, and much, much more.

As one tech executive recently described it to me, all software design assumes that all data should be collected, and most of this occurs without the user's knowledge.

All roads to economic and social participation now lead through surveillance capitalism's institutional terrain, a condition that has only intensified during these two years of global plague.

The abdication of these spaces to surveillance capitalism has become the meta crisis of every republic because it obstructs solution to all the other crises for which we require information integrity and the sanctity of communications.

The world's liberal democracies now confront a tragedy of the "un-commons" as mission critical information in communication spaces, that most people have assumed to be public, are now owned, operated, and mediated by private commercial interests for profit maximization, while almost entirely unconstrained by public law. No democracy can survive these conditions.

The deficit I describe here reflects a larger pattern. The United States and the world's liberal democracies have thus far failed to construct a coherent political vision of a digital century that advances democratic values, principles, and government, while the Chinese, for example, in contrast, have focused on designing and deploying digital technologies in ways that advance their system of authoritarian rule.

This failure left a void where democracy should be, leaving our citizens now to march naked into the third decade of surveillance capitalism without the rights, laws, and institutions necessary for a democratic digital future.

Instead, we have stumbled into an accidental dystopia, a future that we did not and would not choose. In my view, we must not and cannot allow this to be our legacy.

Survey evidence, some of which has already been referred to here, now shows that Americans are moving ahead of their lawmakers in a massive rupture of faith with these companies.

We see extraordinary majorities calling for action to curb the unaccountable social power of these firms, a realization that the emperor of surveillance capitalism not only has no clothes, but is dangerous, and a clear sense that human rights, the durability of society, and democracy itself are on the line. What was undiscussable has become discussable. What was settled is now being questioned.

To end, we are still in the very early days of our information civilization. This third decade is a crucial opportunity to build the foundations for a democratic digital century. Democracy may be under siege, but it is, however paradoxically, the kind of siege that only democracy can end.

Thank you so much for your attention.

[The statement of Ms. Zuboff follows:]

HARVARD UNIVERSITY

GRADUATE SCHOOL OF BUSINESS ADMINISTRATION

GEORGE F. BAKER FOUNDATION

SHOSHANA ZUBOFF

*Charles Edward Wilson Professor of Business Administration, Emeritus***PRIVACY MUST FALL****Surveillance Capitalism and the Meaning of Privacy Law After Privacy***Written testimony of*
Professor Shoshana Zuboff*Before the*
Committee on House Administration
U.S. House of Representatives*For the hearing on*
Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors

February 16, 2022

Chair Lofgren, Ranking Member Davis, and members of the Committee, thank you for this opportunity to discuss the challenges of privacy law in a world without privacy.

I have spent forty-three years studying the rise of the digital as an economic force driving our transformation into an information civilization. Over these last two decades, I've observed the consequences as fledgling internet companies morphed into surveillance empires founded on the premise that *privacy must fall* and powered by global operations of behavioral monitoring, analysis, targeting, modification, and prediction that I have called 'surveillance capitalism'.¹

I. A Tragedy of the Uncommons

In this written testimony, I pose the following questions to the Committee on House Administration: What kind of legislative action is required to protect privacy in the aftermath of its wholesale destruction? What is the nature and purpose of privacy law after privacy? While

these questions and their answers beg explanation, I confine myself here to the essential points necessary for meaningful deliberation.

In an information civilization, societies are defined by questions of knowledge — how it is distributed, the authority that governs its distribution, and the power that protects that authority. *Who knows? Who decides who knows? Who decides who decides who knows?* Surveillance capitalists now hold the answers to each question, though we never elected them to govern. They claim the authority to decide ‘who knows’ by asserting ownership rights over human-generated information, and they defend that authority with the power to control critical information spaces, systems, and infrastructures.² On the strength of their surveillance capabilities and for the sake of their surveillance profits, the new empires engineered an anti-democratic *epistemic coup* — a takeover of knowledge and knowing — marked by unprecedented concentrations of knowledge about individual and collective behavior along with the unaccountable power that accrues to such knowledge.

The world’s liberal democracies now confront a tragedy of the ‘un-commons,’ as mission-critical information and communication spaces and functions have been ceded to surveillance capital. Digital territories that most people have assumed to be public are now owned, operated, and mediated by private commercial interests for maximum profit while almost entirely unconstrained by public law. All roads to economic and social participation now lead through surveillance capitalism’s institutional terrain, a condition that has intensified during nearly two years of global plague. The abdication of these spaces to surveillance capitalism has become the meta-crisis of every republic because it obstructs solutions to all other crises. No democracy can survive these conditions.

This third decade demands a reckoning with the most basic questions of the digital century: how do we reinvent the operations and governance of information and communication in ways that sustain and advance democratic values, principles, and aspirations? The liberal democracies skipped this most crucial step at the dawn of the information age, leaving a void that was filled by surveillance capital.

The result is the feeling that we’ve stumbled into a future that we did not and would not choose, one that is increasingly ruled by the antidemocratic and unaccountable power of surveillance capitalism. A sure test of this statement is that when our young people and our artists contemplate the future, they invariably assume the overriding presence of omniscient dystopian power. This must not be our legacy.

I begin this discussion by defining surveillance capitalism as an economic logic that depends upon the destruction of privacy as a condition of its success. I then briefly discuss the historical conditions that enabled this surprising economics to root and flourish. Next, I examine the stages of surveillance capitalism’s development from its origins in the destruction of individual privacy to its current status as a sweeping institutional order vying with democracy over the principles and laws that will govern society. With these elements identified, I consider the legislative and institutional challenges of this third decade and their bearing upon the renewal of privacy as a necessary condition of a democratic digital century.

II. What is Surveillance Capitalism?

Surveillance capitalism maintains core elements of traditional capitalism: private property, market exchange, growth and profit, but these cannot be realized without the technologies and social relations of surveillance. So, here is the startling new economics of surveillance capitalism: Hidden methods of observation secretly extract human experience once considered private and translate it into behavioral data. These methods operate outside of human awareness, robbing actors of the right to know and, with it, the right to combat. In an extraordinary development, these ill-gotten human data are then immediately claimed as corporate property available for manufacture and sales. The theory of surveillance capitalism challenges this property claim and redefines it as theft.

Human data thus extracted join complex supply chains and travel to computational factories, known as “machine learning” or “artificial intelligence,” where they are computed into behavioral predictions and targeting algorithms. Predictions are ultimately sold to business customers in a new kind of market that trades in predictive knowledge of human behavior. These are commodity markets in human futures akin to markets in pork belly futures, or wheat, or oil. Surveillance capitalists sell certainty, which demands data extraction at a massive scale that is impossible to grasp. A leaked 2018 Facebook document provides a glimpse.³ The company describes its “prediction engine” that “ingests trillions of data points every day,” to produce thousands of “models,” and its “prediction service” that churns out “more than 6 million predictions per second.”

Surveillance capitalism developed into a global institutional order in only two decades, in part because of the many ways in which it learned to persuade America and the world of its inevitability. Nevertheless, this institution was and is anything but inevitable. Its success is owed to action and choice. People made it. Chance made it. Ideology, economics, and politics made it.

The year was 2000, when a mere 25% of the world’s information was stored digitally, and a tiny but brilliant Silicon Valley internet startup called Google faced ruin from the financial crisis known as the dotcom bust. Even as Google’s search engine was considered the best, founders Larry Page and Sergey Brin faced extreme pressure from their powerful venture capitalist investors. The company had not yet found a way to turn search into money, and their backers insisted on a fast track to monetization.

Between 2000 and 2001, the Google team stumbled into a series of discoveries that revealed the rich predictive signals embedded in the “data exhaust” left over from users’ search and browsing activities, signals that could be aggregated and analyzed to predict user behavior. This leftover behavioral data was a *surplus*, more than what was required for product improvement. The founders had argued that advertising would corrupt the search experience, but financial emergency created a state of exception, and they suspended their principles.⁴ Advertising became their lifeboat as they learned how to analyze behavioral surplus to predict click-through rates, the solid gold that launched their vast and lucrative online ad markets.

Surveillance is the keystone of this economic foundation. From the start, data scientists and engineers understood that these operations would have to be hidden, lest they risk user rebellion

or lawmakers' anger. Soon, its scientists were inventing ways to surveil and capture behavioral surplus across the internet without leaving a trace, proud of their ability to construct, infer, and deduce user profiles with insights that individuals never chose to disclose — personality, sexual orientation, political leanings ... and much more. Later, the mobile revolution would move these secret extraction activities into the real worlds of everyday life. Such hidden-taking-without-asking is normally characterized as theft, and it is on the strength of this secret theft that 'users' once private lives are transformed into others' proprietary assets.

The discovery of behavioral surplus and the related sciences of inference, computation, modeling, algorithms, prediction and targeting known loosely as 'artificial intelligence' undermine the validity of rational choice theory or the contractual integrity of notice and consent. One may exercise rational choice in the decision to share specific information with a platform, but that information is an insignificant drop in the ocean of surplus that is hunted and captured and delivered to sophisticated machine procedures to produce more surplus. I cannot make a rational choice about what is concealed from me — the known unknown.

Google had been a technology company. Its business plan called for selling search engine licenses to large internet companies and other corporate clients. It even produced a device, the "Google Search Appliance," to help companies locate information in their own databases.⁵ All of that was swept away.

Founder Larry Page laid it out in 2001, shortly after the breakthrough that would change everything. "If we did have a category," Page ruminated, "it would be personal information ... The places you've seen. Communications ... Sensors are really cheap ... Storage is cheap. Cameras are cheap. People will generate enormous amounts of data ... Everything you've ever heard or seen or experienced will become searchable. Your whole life will be searchable."⁶

Instead of selling search to users, Google would achieve revenue growth by searching its users and seizing whatever it found. Escape from financial ruin, it was decided, depended upon turning Google's search engine into a sophisticated surveillance medium for the massive-scale seizure of human-generated data.

Privacy did not disappear, exactly. Instead, it was expropriated from people and concentrated in the corporate domain. Google used its capabilities in surveillance to keep the new economic operations secret. Founders and executives were determined to hide their breakthrough from competitors, but they also feared that users would rebel against corporate mass surveillance. Worst of all was the anxiety that lawmakers might be stirred to action. According to the company's first brand manager, Douglas Edwards, Page opposed anything that might "stir the privacy pot and endanger our ability to gather data." He even questioned the prudence of the legendary electronic ticker display in the company's Mountain View lobby, and its continuous stream of search queries.⁷

Page also wanted to hide the astonishing financial implications of Google's invention. Between 2001, when the new economics of surveillance advertising were first applied, and 2004, when Google went public, its revenues increased by 3,590 percent. This 'surveillance dividend'

established the secret massive-scale extraction of human-generated data as the foundation of a new economic order.

Facebook was Google's first follower. Like Google a few years earlier, its founder Mark Zuckerberg had not found a way to turn popularity into profit. He changed his destiny in 2008 by hiring Sheryl Sandberg as his second in command. Sandberg had joined Google in the breakthrough year of 2001 and became a key leader of the surveillance capitalism advertising revolution. She led the build-out of Google's advertising engine, AdWords, and its AdSense program, which together accounted for most of the company's \$16.6 billion revenues in 2007.⁸

By the mid-2010s, surveillance economics had become the default economic model in the tech sector. Success drew surveillance economics inexorably into the 'normal' economy, where it has continued to migrate and reorder diverse sectors from insurance, retail, banking and finance to agriculture, automobiles, education, healthcare and more. Every product called "smart," and every service called "personalized" are loss leaders for the human data that flow through them. Today every 'app,' no matter how apparently benign, is designed as a data mule, shuttling personal information from devices to the servers at Google, Facebook, and ad tech companies. As one Silicon Valley executive recently described it to me, "The underlying norm of virtually all software and apps design now is data collection. All software design assumes that all data should be collected, and most of this occurs without the user's knowledge." Extraction operations and their supply chains range far beyond their original settings on computers, laptops, and smartphones to cities and villages, buildings and roads, homes and cars — every form of activity in every domain of daily life.

Among the five leading surveillance capitalist corporations — Google, Facebook, Amazon, Apple, and Microsoft — each participates in surveillance advertising and surveillance economics, though the specifics of their business models vary. Google and Facebook are data companies and surveillance-advertising "pure plays" whose revenues derive almost entirely from surveillance advertising markets.⁹ The others have multiple lines of business that include varying configurations of data, services, software, and-or physical products. Despite these distinctions, all five contribute to, benefit from, and build upon surveillance capitalism's institutional strategies, operations, and revenues in conjunction with their complex ecosystems, the ad tech behemoths, the telcos, the internet service providers, and a growing majority of market-based organizations across the commercial universe. It is therefore not surprising that in 2021 the five giants were also five of the six largest publicly traded companies by market capitalization in the world.¹⁰

III. Windfall

Nothing was inevitable. Ours is an accidental dystopia.

Surveillance capitalism is neither a technology nor a corporation nor an executive. It is a political-economic institution that owes its existence to a windfall of unique economic, political, ideological, and material conditions that permitted this extractive economic logic to root and

flourish. I have documented these conditions in detail in other work, and here I shall mention only a few highlights.¹¹

In 1970, three years before Larry Page's birth, the *New York Times Magazine* lent its prestigious pages to "A Friedman Doctrine," the libertarian call to arms giving popular voice to a radical free market world view that would be essential to Page's, and surveillance capitalism's, astounding success.¹² "There is one and only one social responsibility of business," the University of Chicago economist thundered, "to use its resources and engage in activities designed to increase its profits ..."

Friedman was a self-described "extremist" partial to sharp dualisms, absolutes, and unequivocal policy positions that frequently triggered public controversy.¹³ His ideology was forged in the aftermath of World War II as a response to the collectivist nightmares of German and Soviet totalitarianism. As the old central planning enemies receded, new ones took their place: the regulatory powers of the democratic state, its social legislation and welfare policies, labor unions and the institutions of collective bargaining, and principles of equality and justice. These were replaced by the market's version of truth. Growth would be accelerated by unimpeded market competition sustained by supply-side reforms, including comprehensive deregulation, privatization, and lower taxes.

By mid-decade, as the Nixon and then the Ford White House searched for a way out of the stagflation crisis, Professor Friedman advised both Presidents. By 1979 he was economic advisor to Presidential candidate Ronald Reagan, a relationship that endured throughout Regan's presidency. President Reagan and British Prime Minister Margaret Thatcher famously established Friedman's radical free market doctrine as governmental policy. The market must rule. Democratic institutions must recede.

From the start, the internet and its commerce were claimed for Friedman's radical freedom, and the overarching theme of internet-related governmental policy was "self-regulation" for the sake of Friedman-style profit maximization. This ideological zeitgeist dominated those crucial post-World Wide Web years of the mid to late 1990s finding iconic expression in a 1997 Clinton-Gore whitepaper.¹⁴ The Administration's policy vision for "Global Electronic Commerce" begins with its primary principle: "The private sector should lead." The Google founders became the unwitting heirs apparent of the Friedman Doctrine.

The report denigrated to the point of caricature government's role and capabilities in the governance of digital information and communication spaces, insisting on "minimal government involvement or intervention ... Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated ...". The Administration's approach was not only to get out of the way, but to proactively cede whole governance functions to the internet companies. When it came to privacy protections, the whitepaper's prescriptions rested on formulations that even in 1997 were not easily defensible. This shortfall became more dangerous once the science of behavioral surplus extraction, inference, and computation was invented. The Clinton-Gore framework left 'users' naked at the altar of the rational choice theory assumed in the whitepaper's advocacy of privacy protections such as, "market resolution of privacy concerns by empowering individuals to obtain relevant knowledge," "self-regulatory privacy regimes,"

“industry-developed solutions to privacy problems,” and “market driven mechanisms to assure customer satisfaction about how private data is handled.”

By 2000, however, a majority of FTC commissioners, including Chair Robert Pitofsky, concluded that self-regulatory initiatives “cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders ... notwithstanding several years of industry and governmental effort.” In their report to Congress, the Commissioners cited the explosion of secret online tracking and monitoring for chasing eyeballs with new hidden methods like “cookies” and “web bugs.”¹⁵ They noted that a mere 8 percent of popular websites featured a seal of approval from one of the internet industry’s privacy watchdogs, intended as an important mechanism for self-regulation.

The report argued that only federal law could protect online consumers. Proposed stipulations included clear and conspicuous notice of information practices; consumer choice over how personal information is used; individuals’ access to all personal information including rights to correct or delete; and enhanced security of personal information.¹⁶ Even these basic privacy protections would have set America and the world on a different path to the digital century, but history, contingency, and chance had other plans: September 11, 2001.

According to Peter Swire, chief counselor for Privacy in the Clinton Administration and later a member of President Barack Obama’s Review Group on Intelligence and Communication Technologies, “With the attacks of September 11, 2001, everything changed. The new focus was overwhelmingly on security rather than privacy.”¹⁷ The legal provisions debated just months earlier vanished from the conversation more or less overnight, giving way to a new preoccupation with “Total Information Awareness.”

Friedman’s ideology of radical market freedom took care of the supply side, shielding the nascent surveillance capitalist firms from laws that would have curbed the destruction of privacy and all that followed from it. Then, 9/11 thrust the intelligence community, the US government, and, indeed, governments around the world into an unfamiliar demand curve, mobilized by outrage and anxiety. In America, a ‘state of exception’ was invoked to unleash a new human data imperative: velocity and volume at any price. In this new environment “Congress lost interest in regulating information usage in the private sector,” Swire recalls. “Without the threat of legislation, the energy went out of many of the self-regulatory efforts that industry had created.”¹⁸

In the US and across the EU, legislation was quickly put in place that decisively expanded surveillance activities.¹⁹ Instead of federal legislation to outlaw the novel surveillance practices, the new aim was to enrich the conditions for their expansion and application outside constitutional, legal, and regulatory constraints. Yale legal scholar Jack Balkin explained that while the US Constitution inhibits surveillance by government actors, privacy protections for information held in private servers is “limited if not nonexistent.” If the intelligence community was to indulge its obsession to ascertain the future, then it would have to “rely on private enterprise to collect and generate information for it.”²⁰

Google took the lead and in the process surveillance capital was given a free pass to invent, own, and operate the twenty-first century production, concentration, and use of human-generated data. By 2010, former NSA director Mike McConnell publicly acknowledged that collaboration was inevitable noting, “With more than 90 percent” of the physical infrastructure of the web “owned by private industry ... the challenge is to shape an effective partnership with the private sector so information can move quickly back and forth from public to private ...”²¹

IV. Our Accidental Dystopia: Surveillance Capitalism’s Stages of Development

Most of us are whipsawed by each day’s headlines bleating the latest atrocity: the loss of privacy, the spread of disinformation, collective-scale behavioral modification. The issues are siloed, fragmented. We are forever trying to grasp the elephant while fixating on its parts, leaving us in a tangle of disorientation and confusion with little grasp of economic cause and social harm effect. If we have learned anything from this state of affairs, it’s that we cannot fix what we do not understand.

The value of reinterpreting surveillance capitalism as a developing institutional order is that this tower of Babel finally resolves into a coherent picture – linked effects of a unitary process evolving in time. Each stage is defined by more complex economic operations that cause new social harm effects and enable the absorption of new governance functions. Each stage creates the conditions for the next. Each builds on what went before. Seemingly disparate social harms are organically related in time – the effects of economic operations also related in time. This picture alerts us to the ways in which effective remedies for later stage social harms depend upon changing early-stage operational causes. In other words, the durable solutions lie upstream, where this river originates.

Four stages of surveillance capitalism’s institutionalization are visible thus far: Extraction, Expropriation, Exploitation, and Enforcement. I’ll describe them briefly.

Stage One: Extraction

The first stage introduces the secret massive-scale extraction of human generated data, the formative achievement that lays the economic foundation for all that follows. Human-generated data are concentrated in the surveillance capitalist order.

And there is no law to stop it.

Stage Two: Expropriation

In his 1967 dissenting opinion in the Fourth Amendment case of *Warden v. Hayden*, Justice William O. Douglas wrote, “Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses ... Those who wrote the Bill of Rights believed that every individual needs both to communicate with others and to keep his affairs to himself. That dual aspect of privacy means that the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of that sharing.”²²

Douglas's "freedom to select" alerts us to a class of rights that precede privacy, and the enactment of such rights are the proximate cause of privacy. These rights to know are 'epistemic rights,' which in modern democratic societies have been considered inalienable and elemental rights of individuals. With the secret seizure of human data from domains of experience that have long been considered private, the epistemic rights embedded in Douglas's "freedom to select" are expropriated and accumulated as corporate rights. Because privacy is an effect of this "freedom to select," the expropriation of epistemic rights eliminates the privacy choice. This dynamic clarifies the advancement of stage two from concentrations of human data, to concentrations of epistemic rights, to concentrations of privacy, to concentrations of recently private knowledge about people as corporate property.

These concentrations are not metaphorical. They reflect elaborate infrastructures of material and people. For example, a comprehensive review of AI's global institutional structure concludes that the artificial intelligence landscape is almost entirely controlled by "big tech." These firms evangelize AI because they stand to benefit from improvements in their own businesses. Some of the vertical ecosystems have gone global as "scale begets learning through the accumulation of data and increases competitive advantage". The surveillance capitalist giants control the capital, the data, the technologies, the scientists, and the science. They acquire most AI firms and poach most AI talent. Consistent with the structure of concentration in these corporations, the report observes that "Secrecy rather than patenting remains the preferred strategy to protect their research findings."²³

The social harm effects are the wholesale destruction of privacy and the construction of a new axis of inequality defined by the growing gap between 'what I can know and what can be known about me.' At this stage of development, surveillance capitalism governs the production of and access to knowledge about people and society for its own advantage, which establishes its dominance over and information society.

And there is no law to stop it.

Stage Three: Exploitation

Now, growing concentrations of knowledge are transformed into power. "Targeting" is the preferred euphemism as the scale and scope of data feed a range of digital cueing mechanisms engineered to tune, herd, constrain, direct, and condition individual and collective behavior to maximize engagement for maximum predictability and extraction. Operations engineered for profit maximization are systemically biased toward more corrupt and inflammatory content, which is proven to yield higher levels of "engagement."²⁴

These economic operations cause social harm effects across multiple vectors as they produce epistemic chaos. Such chaos begins with the degradation of information integrity, as defactualized content is artificially driven to the center of social discourse by algorithmic targeting engineered for engagement. Such targeting aims to shape behavior through a variety of mechanisms including subliminal cues, engineered social comparisons, psychological microtargeting, rewards and punishments, and more. These mechanisms further intensify inequality as expressed in the growing gap between 'what I can do and what can be done to me,'

degrading the integrity of individual and collective behavior. And as targeting operations mediate information and communication, they erode common sense and produce a more splintered and polarized society.²⁵

The governance functions associated with these harms are illustrated in the *Wall Street Journal's* "Facebook Files," which showed Mr. Zuckerberg's power to play his celestial keyboard, reinforcing or extinguishing the behavior of billions of people. Anger is rewarded or ignored. News stories become more trustworthy or unhinged. Publishers prosper or wither. Political discourse turns uglier or more moderate. People live or die.²⁶

And there is no law to stop it.

Stage Four: Enforcement

At this stage firms begin to enforce governance prerogatives by leveraging their ownership and control of information and communication spaces, systems, and infrastructures. By now the institutional order is sufficiently entrenched to openly vie for governance of mission-critical spheres of democratic capabilities (such as healthcare), but also to openly contest democratic institutions and their elected and appointed officials. The aim now is to absorb political governance functions in an increasingly open showdown over governance.

There have been more frequent sightings of this stage four behavior – Facebook's current threats to withdraw from Europe, Facebook's Oversight Board, the Google-Facebook contest with the Australian parliament. April 2020 brought a showdown between the European Commission and its member governments on the one hand, and Apple and Google on the other. The companies had abruptly introduced a COVID-19 exposure notification protocol for Androids and iPhones that was incompatible with government-supported exposure notification and contact tracing applications already in development. Tense negotiations followed, as democratically elected leaders and government officials tried unsuccessfully to persuade Apple's CEO Tim Cook, Google's Sundar Pichai, and assorted corporate executives to adapt their operating system for the use of European public health authorities and urgent epidemiological research.

And there is no law to stop it.

Surveillance capitalism's whirlwind two-decade developmental journey now reveals itself as one vector of a larger contest between institutional orders. At each developmental stage we see a zero-sum dynamic in which the deepening institutional order of surveillance economics propagates democratic disorder.

This clash of institutional orders clarifies the reason for Congressional action. We have drifted into an accidental dystopia. The only countervailing institutional order capable of obstructing surveillance capitalism's path to dominance is the liberal democratic state. Surveillance capitalism is the younger challenger, but it embodies many unprecedented strengths. And while it is true that democracy is the old and slow incumbent, it brings powerful advantages that are difficult to rival. Chief among these is the legitimate authority and requisite power to make, impose, and enforce the rule of law. What laws must be devised if there is to be any hope of rescuing the digital century for democracy?

V. A Democratic Resurgence

A century ago, the corporate concentration of power was understood as economic power, and owners had all the authority on the strength of their property rights. The harms of concentration fell on people in their economic roles as workers, consumers, and competitors. Decades of contest and collective action eventually produced antitrust laws, but also new charters of rights for workers and consumers, the laws to protect them, and the public institutions charged with their enforcement and governance.

As important as those creations remain today, they do not protect us from the new harms we face. Ours is an accidental dystopia for the many reasons we have reviewed, including these: neither lawmakers nor citizens anticipated the harms that follow when the dominant economic institutional order is founded on the secret extraction of personal human experience once assumed to be private and now transformed into raw material for commercial operations. Nor did we grasp the harms that follow when revenues depend upon making all human behavior more predictable across all domains of everyday life. Nor did we imagine the social degradation unleashed when information and communication spaces are owned, operated, and mediated by an economic system in which information integrity is negatively correlated with revenues.

These conditions illuminate the changing nature of corporate concentration. In the age of surveillance capitalism, corporate power is not only economic but social. Its social harms are not confined to individuals in their roles as workers and consumers. They fall upon ‘users’: a new category of humanity that means all of us, all the time, everywhere. Ours is a young information civilization that has not yet found its footing in democracy because the social harms we face cannot be shoehorned into Cinderella’s 20th century legal slipper. So, now it is **we** who march naked, without the rights, laws, and institutions purpose-built to govern our digital century in the name of democracy.

The tech giants and their fellow travelers have been willing to treat their destructive effects on people and society as collateral damage — the unfortunate but inevitable byproduct of digital technologies employed in perfectly legal economic operations. In April 2020 as the world tried to come to grips with Covid-19, former Google CEO Eric Schmidt, boasted that the pandemic would teach Americans to be “a little bit grateful” for powerful tech companies.²⁷ Other tech executives welcomed what they believed would be the inevitable end of ‘techlash’ thanks to widespread pandemic-induced dependency.

But as we enter the third decade of the digital century, something extraordinary is occurring: the aura of inevitability is giving way to the realization that the emperor is not only naked but dangerous. The data from prominent US attitude surveys suggests a public rupture of faith with surveillance capitalism and the power of its dominant corporations. Instead of a little gratitude there is a lot of anger and dismay.

I will tailor my remarks to just a few of the most recent surveys and the extraordinary majorities that voice dissent over surveillance capitalism’s social harms. As evidenced in the following surveys, the American population is overwhelmingly calling for action to curb the unaccountable

power of surveillance capitalism and its giant protagonists. Americans want an end to the social harms that spin from these corporate orbits with increasing velocity and destructive force. There is a clear sense that human rights, the durability of society, and democracy itself are on the line.

A Knight Foundation/Gallup survey in July 2020 found that 77 percent of adult Americans believe Big Tech companies have too much power.²⁸ Ninety-four percent of respondents were concerned about privacy and 92 percent were concerned about the spread of disinformation and its effects on society. Only 30 percent were concerned about innovation. An Accountable Tech survey in January 2021 found 71 percent of respondents favoring regulatory intervention.²⁹ Eighty-one percent preferred privacy over the benefits of targeted advertising, and 73 percent were opposed to behavioral tracking and personal data collection for the sake of targeted ads. Finally, in significant majorities, respondents were in favor of banning social media companies from boosting extreme content (84 percent) as well as banning the collection of personal data for targeting (81 percent). Another 86 percent favored holding companies legally accountable for boosting violent content on their platforms.

Data published six months later in July 2021 further suggest that the American public no longer accepts the secret massive-scale extraction of human data as either inevitable or desirable. In an extensive US survey commissioned by the Future of Technology Commission, 93 percent of respondents agreed with the following statement: “It should be illegal for private companies to collect information about people without their permission.”³⁰ It was the largest majority in agreement with any statement in this lengthy section of the study.

In 2022, the American public finally may be ready to shout that the emperor has no clothes, redefining illicit data extraction as theft and thus dismantling the keystone of surveillance capitalism’s profits and power: the secret massive-scale extraction of human generated data.

An early vanguard of privacy-oriented scholars feared the internet companies’ concentrated power and corrosive effect on democracy.³¹ It is useful to note that these pioneers now have been joined by a new wave of scholarship mobilized by concerns over the startling concentrations of power in the giant tech firms and their implications for the democratic social order.³²

Where does the widespread rupture of public faith leave us? Democracy is the only countervailing institutional order with the legitimate authority and power to change our course. If the ideal of human self-governance is to survive the digital century, then all solutions point to one solution: *a democratic resurgence*. But instead of the usual laundry lists of remedies, lawmakers need to proceed with a clear grasp of the adversary: a single hierarchy of economic causes and their social harm effects.

While liberal democracies have begun to engage with the challenges of regulating today’s privately owned information spaces, the sober truth is that we need lawmakers ready to engage in a once-a-century exploration of far more basic questions. How should we structure and govern information, connection, and communication in a democratic digital century? What new charters of rights, legislative frameworks and institutions are required to ensure that data collection and use serve the genuine needs of individuals and society? What measures will protect citizens from

unaccountable power over information, whether it is wielded by private companies or governments?

Privacy law after privacy looks like this:

1) ***Interrupt supply by outlawing secret massive-scale extraction of human-generated data.*** We can't rid ourselves of later-stage social harms unless we interrupt and outlaw their foundational economic causes. This means we move beyond the current focus on downstream issues where we argue about content moderation, illegal content, and 'filter bubbles,' as lawmakers and citizens stamp their feet at recalcitrant executives who have already claimed these unceasing data flows as their property. Downstream is where the companies want us to be, so consumed in the details of the property contract that we forget the real issue, which is that their property claim itself is illegitimate. The edifice of surveillance economics is built on this foundation of sand. Every argument that begins with 'data' is an argument that we have already lost. Like a magician's rabbit, the endless, and often pointless, downstream discussions direct our attention away from the mechanics of the trick. It's like arguing over the details of a seven-year old's factory contract instead of outlawing child labor. Similarly, structural solutions like "breaking up" the tech giants may be valuable in some cases, but they will not affect the underlying economic operations of surveillance capitalism.

Instead, we need to focus laser-like on the bedrock of surveillance economics, which is the secret extraction of human data from realms of life until recently assumed as "private." Remedies that focus on regulating and eliminating extraction are content neutral. They do not threaten freedom of expression. Instead, they liberate social discourse and information flows from the "artificial selection" of profit-maximizing commercial operations that allow for misinformation with no regard for integrity. They restore the sanctity of social communications and individual expression.

No secret extraction means no illegitimate concentrations of knowledge about people. No concentrations of knowledge mean no targeting algorithms. No targeting means that corporations can no longer control and curate information flows and social speech or shape human behavior to favor their interests. Regulating and outlawing extraction would eliminate the surveillance dividend and with it the financial incentives for surveillance, opening the competitive landscape to new forms of information capitalism that reunite the digital technologies with the real needs of people and society, as data collection is tied to fundamental rights and data use is tied to the public good.

2) ***New conditions summon new rights.*** A democratic information civilization cannot progress without new charters of *epistemic rights*. Citizens of democratic societies have regarded personal experience as inseparable from the individual: inalienable. It follows that the right to know about one's own personal experience has been considered elemental — bonded to each of us like a shadow. My epistemic rights are the cause of which my privacy is the effect. We each decide if and how our experience is shared, with whom, and for what purpose.

Justice Douglas's "freedom to select" is the elemental epistemic right to decide who knows us, how, when, and to what purpose. It is the right from which cause from which all privacy flows.

For example, as the natural bearer of such rights, I do not give Amazon's facial recognition system the right to know if I am afraid or happy. I do not give the corporation the right to exploit my fear for targeting and behavioral prediction that benefit others' commercial objectives. It's not simply that my feelings are not for sale, it's that my feelings are unsale-able because they are inalienable. Though I do not give Amazon my fear, they take it from me anyway, just another data point in the trillions gathered that day.

New legal rights are crystalized in response to the changing conditions of life. Justice Brandeis' commitment to privacy rights, for example, was stimulated by the spread of photography and its ability to invade and steal what was regarded as private. In 1890 he wrote, "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."

Our elemental epistemic rights are not codified in law because until now they have not come under systematic threat, any more than we have laws to protect our rights to stand up or sit down or yawn. But the surveillance capitalists have declared their "right to know" our lives, mobilizing pervasive surveillance at a scale and depth of intimacy that beggar imagination, while claiming the right to own and profit from that knowledge. Thus dawns a new age, founded on and shielded by the false inevitability of surveillance capitalism. Now the once taken-for-granted right to know and to decide who knows 'about me' must be codified in law and protected by democratic institutions, if it is to exist at all.

3) ***Unprecedented harms demand unprecedented solutions.*** Just as new conditions of life reveal the need for new rights, the unprecedented harms of the epistemic coup require purpose-built solutions. This is how law evolves, growing and adapting from one era to the next — Brandeis's "eternal youth."

A mature democratic information society will require independent trustworthy public oversight institutions that hold the market and the state to account in the knowledge that the solution to surveillance capitalism is not a Big Brother state. These institutions are dedicated to a democratic digital future: transparent, governed by the rule of law, immune to political interference, and empowered with the budgetary, technological, and human resources necessary to oversee and enforce the availability and integrity of information for people and democracy.

4) ***Interrupt and outlaw demand for illicit data collection.*** Solutions that interrupt illicit data supply are complimented by solutions that interrupt demand by disrupting the financial incentives that reward surveillance economics. We can outlaw markets that trade in human futures because we have seen their antihuman, antisocial, and antidemocratic harms. This is not a radical prospect. Democratic societies have outlawed other markets that produce reliably dangerous consequences: Markets that trade in human beings were outlawed, even when they supported whole economies. We outlaw markets that trade in human organs and babies because they inflict damage on people and society.

When it comes to privacy law after privacy, the digital century forces us to choose: *We may be a surveillance society, or we may be a democracy, but we cannot be both.* The liberal democracies must take the lead because they have the power and legitimacy to do so. But they should know that their allies and collaborators include the people of every society struggling against the double insult of an accidental dystopian future. We have a democratic digital century to build, and there is no time to waste.

Notes

- ¹ Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89, <https://doi.org/10.1057/jit.2015.5>; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).
- ² Pascale Davies, "Meta Warns It May Shut down Facebook and Instagram in Europe," *Euronews*, February 7, 2022, <https://www.euronews.com/next/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe-over-data-transfer-issues>.
- ³ Sam Biddle, "Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document," *The Intercept*, April 13, 2018, <https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/>.
- ⁴ Sergey Brin and Lawrence Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," *Computer Networks and ISDN Systems*, Proceedings of the Seventh International World Wide Web Conference, 30, no. 1 (April 1, 1998): 107–17, [https://doi.org/10.1016/S0169-7552\(98\)00110-X](https://doi.org/10.1016/S0169-7552(98)00110-X).
- ⁵ Andrew Zipern, "Technology Briefing | Internet: Google Enters Corporate World," *The New York Times*, February 12, 2002, sec. Business, <https://www.nytimes.com/2002/02/12/business/technology-briefing-internet-google-enters-corporate-world.html>.
- ⁶ Douglas Edwards, *I'm Feeling Lucky: The Confessions of Google Employee Number 59* (New York: Houghton Mifflin Harcourt, 2011), 291.
- ⁷ Edwards, 340–45.
- ⁸ Jessi Hempel, "Sheryl Sandberg: Facebook's New Number Two," *CNN Money*, April 11, 2008, https://money.cnn.com/2008/04/11/technology/facebook_sandberg.fortune/.
- ⁹ "Google: Ad Revenue 2001-2020," Statista, n.d., <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>; "Facebook: Annual Segment Revenue 2020," Statista, n.d., <https://www.statista.com/statistics/267031/facebooks-annual-revenue-by-segment/>.
- ¹⁰ Jenna Ross, "The Biggest Companies in the World in 2021," *Visual Capitalist*, June 10, 2021, <https://www.visualcapitalist.com/the-biggest-companies-in-the-world-in-2021/>.
- ¹¹ Zuboff, *The Age of Surveillance Capitalism*.
- ¹² Milton Friedman, "A Friedman Doctrine-- The Social Responsibility Of Business Is to Increase Its Profits," *The New York Times*, September 13, 1970, sec. Archives, <https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html>.
- ¹³ Angus Burgin, *The Great Persuasion: Reinventing Free Markets since the Depression* (Cambridge, MA: Harvard University Press, 2012), chap. 5.
- ¹⁴ President William J. Clinton and Vice President Albert Gore, Jr., "A Framework For Global Electronic Commerce" (The White House, n.d.), <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html>.
- ¹⁵ Robert Pitofsky et al., "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress," *Federal Trade Commission*, May 1, 2000, 35.
- ¹⁶ Pitofsky et al. The report's legislative proposals set forth a basic level of privacy protection for all visits to consumer-oriented commercial websites to the extent not already provided by the

Children's Online Privacy Protection Act (COPPA). Such legislation would set out the basic standards of practice governing the collection of information online and provide an implementing agency with the authority to promulgate more-detailed standards pursuant to the Administrative Procedure Act, including authority to enforce those standards. All consumer-oriented commercial websites that collect personal identifying information from or about consumers online, to the extent not covered by the COPPA, would be required to comply with the four widely accepted fair information practices: (1) Notice. Websites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through nonobvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. (2) Choice. Websites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). (3) Access. Websites would be required to offer consumers reasonable access to the information a website has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or delete information. (4) Security. Websites would be required to take reasonable steps to protect the security of the information they collect from consumers.

¹⁷ Peter Swire, "The Second Wave of Global Privacy Protection: Symposium Introduction," *Ohio State Law Journal* 74, no. 6 (2013): 845, <https://kb.osu.edu/handle/1811/71601>.

¹⁸ Swire, 846.

¹⁹ Paul M. Schwartz, "Systematic Government Access to Private-Sector Data in Germany," *International Data Privacy Law* 2, no. 4 (November 1, 2012): 230, 235, <https://doi.org/10.1093/idpl/ips026>; W. Gregory Voss, "After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change," *Business Lawyer* 71, no. 1 (January 6, 2016), <https://papers.ssrn.com/abstract=2711996>; Mark Scott, "Europe, Shaken by Paris Attacks, Weighs Security With Privacy Rights - The New York Times," *New York Times - Bits Blog*, November 18, 2015, <https://web.archive.org/web/20151119015821/https://bits.blogs.nytimes.com/2015/11/18/europe-shaken-by-paris-attacks-weighs-security-with-privacy-rights/>; Frank A. Pasquale, "Privacy, Antitrust, and Power," *George Mason Law Review* 20, no. 4 (2013): 1009–24; Pasquale, 1009–24; Alissa J. Rubin, "Lawmakers in France Move to Vastly Expand Surveillance," *The New York Times*, May 5, 2015, sec. World, <https://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html>; Georgina Prodhan and Michael Nienaber, "Merkel Urges Germans to Put aside Fear of Big Data," *Reuters*, June 9, 2015, sec. Technology News, <https://www.reuters.com/article/us-germany-technology-merkel-idUSKBN0OP2EM20150609>.

²⁰ Jack Balkin, "The Constitution in the National Surveillance State," *Minnesota Law Review* 93, no. 1 (2008), <https://openyls.law.yale.edu/handle/20.500.13051/1545>.

²¹ Mike McConnell, "Mike McConnell on How to Win the Cyber-War We're Losing," *The Washington Post*, February 28, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html>.

²² "WARDEN, MARYLAND PENITENTIARY, Petitioner, v. Bennie Joe HAYDEN,," Cornell Law School - Legal Information Institute, n.d.,

<https://www.law.cornell.edu/supremecourt/text/387/294>.

²³ Michael G. Jacobides, Stefano Brusoni, and Francois Candelon, “The Evolutionary Dynamics of the Artificial Intelligence Ecosystem,” *Strategy Science* 6, no. 4 (December 2021): 412–35, <https://doi.org/10.1287/stsc.2021.0148>.

²⁴ For example, Soroush Vosoughi, Deb Roy, and Sinan Aral, “The Spread of True and False News Online,” *Science* 359, no. 6380 (March 9, 2018): 1146–51, <https://doi.org/10.1126/science.aap9559>; Laura Edelson et al., “Understanding Engagement with U.S. (Mis)Information News Sources on Facebook,” in *Proceedings of the 21st ACM Internet Measurement Conference* (New York, NY, USA: Association for Computing Machinery, 2021), 444–63, <https://doi.org/10.1145/3487552.3487859>.

²⁵ For example, Fernando P. Santos, Yphtach Lelkes, and Simon A. Levin, “Link Recommendation Algorithms and Dynamics of Polarization in Online Social Networks,” *Proceedings of the National Academy of Sciences* 118, no. 50 (December 14, 2021), <https://doi.org/10.1073/pnas.2102141118>; Ro’ee Levy, “Social Media, News Consumption, and Polarization: Evidence from a Field Experiment,” *American Economic Review* 111, no. 3 (March 2021): 831–70, <https://doi.org/10.1257/aer.20191777>.

²⁶ “The Facebook Files,” *Wall Street Journal*, October 1, 2021, sec. Tech, <https://www.wsj.com/articles/the-facebook-files-11631713039>.

²⁷ Theodore Schleifer, “Google’s Former CEO Hopes the Coronavirus Makes People More ‘Grateful’ for Big Tech,” *Vox*, April 14, 2020, <https://www.vox.com/recode/2020/4/14/21221141/coronavirus-eric-schmidt-google-big-tech-grateful>.

²⁸ “American Views 2020: Trust, Media and Democracy” (Gallup and Knight Foundation, August 4, 2020), <https://knightfoundation.org/reports/american-views-2020-trust-media-and-democracy/>.

²⁹ “America’s Views on Surveillance Advertising” (Accountable Tech, n.d.), <https://accountabletech.org/research/surveillance-advertising/>.

³⁰ “Poll: Nine out of Ten Voters Support Strong Online Privacy Protections While Eight Out of Ten Strongly Support Holding Social Media Companies More Accountable for ‘Illegal and Harmful Content’ Posted on Their Sites,” *Future of Tech Commission*, September 23, 2021, <https://www.futureoftechcommission.org/press-release-launch-poll>.

³¹ Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” *Vanderbilt Law Review* 52, no. 6 (1999): 1607, <https://doi.org/10.2139/ssrn.205449>; Peter Swire, “Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce,” *Department of Commerce*, 1997, <https://doi.org/10.2139/ssrn.11472>; Dennis D. Hirsch, “The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?,” *Seattle University Law Review* 34, no. 2 (February 8, 2011): 439, <https://papers.ssrn.com/abstract=1758078>.

³² See for example Dina Srinivasan, ed., “The Antitrust Case Against Facebook: A Monopolist’s Journey Towards Pervasive Surveillance in Spite of Consumers’ Preference for Privacy,” *Berkeley Business Law Journal* 16, no. 1 (2019): 39–101.

The CHAIRPERSON. Thank you very much, Professor.
Let me call now on Ms. Fitzgerald for her testimony for five minutes.

STATEMENT OF CAITRIONA FITZGERALD

Ms. FITZGERALD. Thank you, Chairperson Lofgren, Ranking Member Davis, and Members of the Committee. Thank you for holding this important hearing and the opportunity to testify today.

I am Caitriona Fitzgerald, Deputy Director at the Electronic Privacy Information Center, or EPIC.

EPIC is an independent, nonprofit research organization in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the Information Age. For over 25 years, EPIC has been a leading advocate for privacy in both the public and private sectors.

The United States faces a data privacy crisis. Large and powerful technology companies invade our private lives, spy on our families, and gather the most intimate details about us for profit. These companies have more economic and political power than many countries and States.

Through a vast, opaque system of databases and algorithms we are profiled and sorted into winners and losers based on data about our health, finances, location, race, and other personal information.

Private companies are not the only problem. Government agencies have also dramatically increased the collection and use of personal data, often purchased, or obtained from those same private companies, while failing to address the significant risks to privacy and cybersecurity.

The impact of this uncontrolled data collection and use by both private companies and the government is especially harmful for marginalized communities, fostering systemic inequities.

These industries and systems have gone unregulated for more than two decades, and this is where it has left us. The system is broken. Technology companies have too much power and individuals have too little.

To restore the balance, we need comprehensive baseline privacy protections for every person in the United States, changes to the business models that have led to today's commercial surveillance systems, and limits on government access to personal data. Most crucially, we need strong enforcement of privacy protections.

In my written statement I go into detail about the crisis we face and the elements of a strong privacy law, but I want to focus here on the importance of enforcement.

Without strong enforcement, many businesses will simply ignore privacy laws and accept the small risk of an enforcement action as a cost of business, as we have seen with privacy laws enacted in Europe and in several States.

Strong enforcement must include a private right of action. This is not new. Congress included private rights of action in the Cable Communications Privacy Act, the Video Privacy Protection Act, FCRA, TCPA, and the Driver's Privacy Protection Act. The statutory damages set in those privacy laws are not large in individual cases, but they really provide powerful incentives for companies to comply with privacy laws.

Strong enforcement also requires Congress to establish an independent data protection agency, or a DPA. The United States is one of the few democracies in the world that does not have a data protection agency. U.S. companies are leaders in technology, and the U.S. Government should be a leader in technology policy.

When you think about the omnipresence of technology in our lives and our economy, it seems obvious that we should have Federal agencies dedicated to overseeing and regulating it.

A data protection agency could promote innovation and competition while protecting privacy by setting rules that help level the playing field for smaller technology companies who currently struggle to compete with tech giants.

A DPA could also be a central authority within the Federal Government on privacy issues. We saw a glaring example of agency failure to properly consider privacy risks of data collection just this month. The IRS sparked outrage after a report surfaced that it had contracted with third-party vendor ID.me to require taxpayers to submit to facial recognition to access tax records online.

Thankfully, following pressure from advocates and Members of Congress, the IRS backtracked, but this contract should have never been signed in the first place. A DPA could ensure that privacy is carefully considered when agencies are weighing contracts like this.

There is broad support for this idea. A recent Data for Progress poll showed that 78 percent of Americans across the political spectrum support establishing a data protection agency.

The good news is that Congress, and indeed this Committee, has a strong bill before it that would restore privacy online for Americans.

The Online Privacy Act, filed by Chairperson Lofgren and Representative Eshoo, is a comprehensive framework that would place strict limits on the collection and use of personal data, extend civil rights protections online, and establish strong enforcement mechanisms via a private right of action and the creation of a U.S. data privacy agency.

EPIC recommends swift action on the Online Privacy Act. There is widespread bipartisan agreement that we need a Federal privacy law. It is time for Congress to act.

Thank you for the opportunity to testify today.

[The statement of Ms. Fitzgerald follows:]



Statement of Caitriona Fitzgerald

Deputy Director, Electronic Privacy Information Center (EPIC)

Hearing on "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors"

Before the

House Committee on House Administration
United States House of Representatives

February 16, 2022

Chair Lofgren, Ranking Member Davis, and members of the Committee, thank you for the opportunity to testify today concerning the privacy risks from Big Data and the need for reform in both the public and private sectors. My name is Caitriona Fitzgerald, Deputy Director at the Electronic Privacy Information Center, or EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For over 25 years, EPIC has been a leading advocate for privacy in both the public and private sectors. In 2020, EPIC released *Grading on a Curve: Privacy Legislation in the 116th Congress*,¹ setting out the key elements of a privacy law.

The United States faces a data privacy crisis. Large and powerful technology companies invade our private lives, spy on our families, and gather the most intimate details about us for profit. These companies have more economic and political power than many countries and states. Through a vast, opaque system of databases and algorithms, we are profiled and sorted into winners and losers based on data about our health, finances, location, gender, race, and other personal information. The impacts of these commercial surveillance systems are especially harmful for marginalized and multi-marginalized communities, fostering discrimination and inequities in employment, government services, health and healthcare, education, and other life necessities.

These industries and systems have gone unregulated for more than two decades. And the result has been uncontrolled data collection, large scale data breaches, and an ecosystem dependent on a few large commercial surveillance platforms. And the enormity of the challenge we face is only going to grow. Americans have no meaningful choice in limiting the collection and use of their personal data online; and they can't simply "log off" services that have become central to our modern society. The more we depend on online platforms to carry out our most basic and essential activities, the more important it is to ensure that those systems are secure and do not undermine our rights to privacy, autonomy, and equity. We need comprehensive, baseline privacy protections for every person in the United States, changes to the business models that have led to today's commercial surveillance systems, limits on government access to personal data, and strong enforcement of privacy protections.

In my testimony today I will discuss (1) the problems we face today due to the failure of policymakers in the United States to create adequate data protection standards; (2) the current state of privacy law in the U.S.; and (3) what a comprehensive approach to data protection and privacy in the United States should look like. EPIC recommends that Congress enact a privacy law that: (1) limits the collection and use of personal data; (2) prohibits discriminatory uses of data; (3) requires algorithmic fairness and accountability; (4) bans manipulative design and unfair marketing practices; (5) limits government access to personal data; (6) provides for a private right of action; (6) preserves states' rights to enact stronger provisions; and (7) establishes a federal data protection agency to enforce these new rules.²

¹ EPIC, *Grading on a Curve*, <https://epic.org/documents/grading-on-a-curve/>.

² Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Justice in the United States* (2021), <https://epic.org/wp-content/uploads/2022/01/Privacy-and-Digital-Rights-For-All-Framework.pdf>.

I. The United States' Data Privacy Crisis

A. Unfettered Data Collection and Exploitation Harms Autonomy and Democracy

The lack of a comprehensive U.S. privacy law threatens individual autonomy and undermines our democratic institutions and national security. Without clear and enforceable data protection rules, there has been widespread overcollection, abusive data practices, and targeting that threatens our rights and institutions. Robust data privacy standards are essential to ensure the protection of human rights, human dignity, and the healthy functioning of our democracy.

Due to the failure of policymakers in the United States to create adequate data protection standards, rather than innovating around privacy-protective ways to advertise, the business models of advertising firms were permitted to grow unencumbered into corporate surveillance systems driven by collecting and commodifying every tiny bit of personal data about us.³ These firms track us across our devices and all over the internet, building detailed profiles about us simply so they can target us with more ads, at the cost of exposing us to ever-increasing risks of breaches, data misuse, manipulation, and discrimination.⁴

Cross-site and cross-device tracking is one reason why the notice-and-consent approach does not work when it comes to privacy. The intricacies and breadth of the commercial surveillance industry are impossible for the vast majority of Internet users to fully grasp. In 2020, The Markup found that one-third of websites they surveyed contained Facebook's tracking pixel, which allows Facebook to identify users (whether or not they are logged into Facebook) and connect those website visits to their Facebook profile.⁵ The Markup also scanned hundreds of websites on sensitive topics and discovered an alarming amount of tracking, including:

- a state agency page on how to report child abuse sending data about its visitors to six ad tech companies;
- WebMD and Everyday Health sending visitor data to dozens of marketing companies; and
- Eighty U.S. abortion providers whose sites included third-party trackers, some of which sent data to Facebook to be connected to user profiles.⁶

These trackers collect millions of data points each day that are then sold or transferred to data brokers, who combine them with other data sources linked to us to build invasive profiles. Sometimes these profiles are used to target people with "personalized" advertisements that stalk them across the web, and in other instances the data profiles are fed into secret algorithms used

³ See generally Shoshana Zuboff, *The Age of Surveillance Capitalism*, Profile Books (2019).

⁴ See Consumer Federation of America, *Factsheet: Surveillance Advertising: How Does the Tracking Work?* (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.

⁵ Julia Angwin, *What They Know... Now*, The Markup (Sept. 22, 2020), <https://themarkup.org/blacklight/2020/09/22/what-they-know-now>.

⁶ Aaron Sankin and Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020), <https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites>.

to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs.⁷

This expansive network of surveillance, profiling, and data extraction is creepy and exploitative, but it has also been weaponized in ways that undermine our political systems and public discourse. The Cambridge Analytica case⁸ provided a clear illustration of the ways that limitless data collection and retention threatens election integrity and our democratic institutions.⁹ When personal data is collected and used to refine, propagate, and amplify hate, extremism, and disinformation, that threatens our self-determination, our elections, and our democracy. Just as advertising companies use profiles about us to manipulate us into purchases, so too can they manipulate our views by filtering the content we see.¹⁰

When Congress was considering consumer privacy legislation in the 1990s, the problem was new and emerging.¹¹ But since then, data collection has grown unchecked for over two decades and it is now beyond a crisis. In poll after poll, Americans say they want privacy. In a survey recently conducted by the Future of Technology Commission, a staggering 86% of Americans agreed that "it should be illegal for private companies to sell or share information about people no matter what" and only 46% agreed that it would be okay for companies to "sell consumers' data as long as they are transparent about how the data is used and make it clear to consumers."¹² In a Morning Consult poll last year, more than 4 in 5 voters said Congress should prioritize privacy legislation.¹³ Congress needs to address this crisis now.

B. Government Use of Personal Data

The commercial exploitation of personal data is not the only threat to privacy. Government agencies have also dramatically increased their collection and use of personal data

⁷ See EPIC, *Data Brokers*, <https://epic.org/issues/consumer-privacy/data-brokers/>.

⁸ Robinson Meyer, *The Cambridge Analytica Scandal, in Three Paragraphs*, *The Atlantic* (Mar. 20, 2018), <https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/>.

⁹ See e.g. Corin Faife and Alfred Ng, *After Repeatedly Promising Not to, Facebook Keeps Recommending Political Groups to Its Users*, *The Markup* (June 24, 2021), <https://themarkup.org/citizen-browser/2021/06/24/after-repeatedly-promising-not-to-facebook-keeps-recommending-political-groups-to-its-users>; Heidi Schlumpf, *Pro-Trump group targets Catholic voters using cellphone technology*, *Nat'l Catholic Reporter* (Jan. 2, 2020), <https://www.ncronline.org/news/parish/pro-trump-group-targets-catholic-voters-using-cell-phone-technology>; Sam Schechner, Emily Glazer, and Patience Haggin, *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, *Wall Street Journal* (Oct. 10, 2019), <https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889>.

¹⁰ Colin Lecher and Leon Yin, *One Year After the Capitol Riot, Americans Still See Two Very Different Facebooks*, *The Markup* (Jan. 6, 2022), <https://themarkup.org/citizen-browser/2022/01/06/one-year-after-the-capitol-riot-americans-still-see-two-very-different-facebook>.

¹¹ See *Hearing on S. 809: The Online Privacy Protection Act of 1999*, S. Comm. on Commerce, Sci. and Trans., Subcomm. on Communications (July 27, 1999) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://archive.epic.org/privacy/internet/EPIC_testimony_799.pdf ("For those who are willing to look closely, there is little indication that self-regulation is working. Privacy policies read more like warning notices and disclaimers.")

¹² Benson Strategy Group, *Future of Tech Commission: Tech Attitudes Survey* (July 20, 2021 - July 29, 2021), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_topline_c1-1.pdf.

¹³ Sam Sabin, *States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data* (Apr. 27, 2021), <https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/>.

while failing to address the significant risks to privacy and cybersecurity posed by modern data systems. Agencies are far behind where they need to be in terms of securing, protecting, and properly minimizing data. The lack of up-to-date rules has led to a default presumption of broad collection and use without necessary protections. The two principal statutes that regulate the federal government's use of personal data, discussed below, were passed twenty and forty-eight years ago.

We saw a glaring example of agency failure to properly consider privacy risks of data collection just this month. Reports that the Internal Revenue Service had contracted with third-party vendor ID.me for identity verification, requiring taxpayers to submit to facial recognition identification in order to access tax records online, sparked immediate controversy.¹⁴ The plan would have forced individuals to submit biometric data to ID.me, who would have held on to that data for a minimum of seven years. Following pressure from advocates and members of Congress, the IRS announced last week that it was reversing course and will not go through with the plan to require individuals to use the privacy identity verification service ID.me to access the IRS website.¹⁵

And government agencies are especially vulnerable to data breaches. A recent Department of Homeland Security Inspector General report found that Customs and Border Protection (CBP) failed to safeguard pictures of travelers obtained for a facial recognition pilot program.¹⁶ 184,000 facial images were exposed in a data breach of a CBP subcontractor, Perceptics, LLC. The Inspector General found that the CBP failed to undertake sufficient information security practices to prevent Perceptics from obtaining the data.

Rashida Richardson has outlined best practices for government procurement of data-driven technologies.¹⁷ Many of these solutions could be implemented without legislative or regulatory action.

C. Self-Regulatory Approaches Have Failed Time and Again to Protect Privacy

Congress should not need further evidence to prove that industry self-regulation does not work when it comes to personal data – it has had nearly three decades to succeed, but instead had led us to the crisis we face today.¹⁸

¹⁴ Drew Harwell, *IRS plan to scan your face prompts anger in Congress, confusion among taxpayers*, Wash. Post (Jan. 28, 2022), <https://www.washingtonpost.com/technology/2022/01/27/irs-face-scans/>.

¹⁵ Alan Rappeport and Kashmir Hill, *I.R.S. to End Use of Facial Recognition for Identity Verification*, N.Y. Times (Feb. 7, 2022), <https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html>.

¹⁶ Joseph Cuffari, Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020).

¹⁷ Richardson, Rashida, *Best Practices for Government Procurement of Data-Driven Technologies* (May 2021), available at <https://ssrn.com/abstract=3855637>.

¹⁸ See Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States* (Oct. 2011), <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>; see also Center for Digital Democracy and U.S. PIRG, *Cookie Wars, Real-Time Targeting, and Proprietary Self Learning Algorithms: Why the FTC Must Act Swiftly to Protect Consumer Privacy*, FTC Privacy Roundtables – Comment, Project No. P095416 (Nov. 4, 2009).

In November 1999, the FTC and Department of Commerce announced the formation of the Network Advertising Initiative (NAI), shortly after DoubleClick, an online target advertising company, was the subject of an FTC investigation. Less than a year later and with little involvement from consumer and privacy groups, the self-regulatory NAI principles were publicized.¹⁹ The NAI standards were unsurprisingly weak. NAI members could transfer information between themselves to an unlimited degree, so long as it is used for advertising. No meaningful enforcement mechanism was incorporated.

Around the same time, the World Wide Web Consortium (W3C) released the Platform for Privacy Preferences (P3P) protocol.²⁰ P3P was a complex and confusing protocol made it more difficult for Internet users to protect their privacy.

Despite stating in a report to Congress in May 2000 that self-regulatory programs fell “well short” of expectations,²¹ the Federal Trade Commission itself released self-regulatory principles in 2009 and again in 2012.²² The 2009 principles sparked the creation of the Digital Advertising Alliance (DAA), which was comprised of industry associations. The DAA promoted weak privacy standards with little enforcement, rubber stamping existing business practices.

Most recently, the Digital Advertising Alliance has promoted its self-regulatory principles,²³ which involve “opt-out” models that are inscrutable and hard for average users to navigate. These systems are designed in every way possible to push people away from privacy protections, to give the appearance of user “control,” but in fact to prevent individuals from exercising any agency over what is done with their data.

None of these self-regulatory systems have worked. They simply cement the existing harmful business practices that form surveillance capitalism. It is past time to move away from self-regulation.

D. Corporate Surveillance is Especially Harmful to Marginalized Communities

The monetization of Americans’ personal data has an acute impact on marginalized communities.²⁴ Invasions of privacy deprive people of opportunities and they perpetuate

https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00013/544506-00013.pdf.

¹⁹ See Letter from EPIC to S. Comm. on Commerce (July 28, 2000), https://archive.epic.org/privacy/internet/NAI_letter.html.

²⁰ EPIC, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (June 2000), <https://archive.epic.org/reports/pretypoorprivacy.html>.

²¹ Fed. Trade Comm’n, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report To Congress* 35 (2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>.

²² Fed. Trade Comm’n, FTC Staff Report: *Self-regulatory Principles For Online Behavioral Advertising: Tracking Targeting, And Technology* (Feb. 2009); Fed. Trade Comm’n, *Protecting Consumer Privacy In An Era Of Rapid Change: Recommendations For Businesses And Policymakers* (Mar. 2012).

²³ Digital Advertising Alliance, DAA Self-Regulatory Principles, <https://digitaladvertisingalliance.org/principles>.

²⁴ See *Protecting Consumer Privacy in the Age of Big Data*, 116th Cong. (2019), H. Comm. on the Energy & Comm., Subcomm. on Consumer Protection and Comm. (Feb. 26, 2019) (testimony of Brandi Collins-Dexter, Color of Change),

systemic inequities in our society. We have all had the experience of being creeped out by an ad targeted at us – many people assume that companies like Facebook must be using the microphones on our phones to listen to us because the ads are so often related to something we just had a conversation about. They are not really listening to us, but the reality is even creepier – they do not need to hear us to know what we are saying or thinking because that is how much data they are collecting about us – the websites we visit, where we are going, who our friends are, and what those friends are reading and doing.²⁵ They are tracking so many data points about us that it really seems like they are listening to us.

For some people, that means being creeped out by an ad. But for marginalized communities, it can often mean not being shown ads for housing or job openings, depriving individuals of life opportunities, and perpetuating systemic inequities in our society.

These data practices threaten individual privacy and autonomy, and companies have proven time and again that they cannot police themselves. Rather than continuing to tweak a system that demonstrably does not work, this problem requires a legislative and regulatory solution.

II. Current Law is Inadequate to Protect Individual Privacy and our Democracy

A. Federal Agencies are Subject to the Privacy Act and E-Government Act

The Privacy Act of 1974²⁶ was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. Executive departments, military departments, independent regulatory agencies, and government-controlled corporations are all covered by the Privacy Act. It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it includes a private right of action, allowing individuals to sue the government for violating the Privacy Act's provisions.

The important purposes of the Privacy Act have been undermined over the last three decades by the numerous and broad exceptions asserted by most agencies. These exceptions (as well as the practical difficulties involved with maintaining and regulating such a vast system of databases) mean that individual privacy is not often as carefully protected as the drafters of the Privacy Act might have liked. Since "records," "systems of records" and "agencies" are narrowly defined, the Act may not cover many types of databases and data-gathering activities. Also, there are certain exceptions given for "law enforcement purposes." Finally, the "routine use" exception

<https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Brandi%20Collins%20Dexter%2002.26.2019.pdf>.

²⁵ Elec. Frontier Foundation, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance* (2019), <https://www EFF.org/wp/behind-the-one-way-mirror>.

²⁶ 5 U.S.C. § 552a.

allows government agencies to disclose individually identifiable information simply by stating their plans to disclose that type of information when they create or alter the database.

The Privacy Act simply defines “routine use” as “the use of such record for a purpose which is compatible with the purpose for which it was collected.”²⁷ Note that a routine use does not have to be a purpose identical to the purpose for which the record was collected, only a compatible purpose. This phrasing can often lead to mission creep for a system of records, in which the routine uses for a particular database gradually increase until its scope is far greater than its originally stated goals.²⁸

The rights provided for under the Privacy Act have also been severely curtailed by a series of misguided court decisions. In 2004, the Supreme Court ruled that individuals whose data is misused by a federal agency are not entitled to the statutory damages that the Privacy Act is intended to provide, but must instead prove actual damages.²⁹ In 2012, the Court ruled that individuals cannot recover damages under the Privacy Act for mental and emotional distress, even when an agency wrongly discloses highly sensitive information like a person’s HIV status.³⁰ These decisions have not only made it exceptionally difficult for individuals to obtain relief for the misuse of their personal information by federal agencies; they have also weakened a key incentive for agencies to comply with the Privacy Act in the first place.

The lesson from the Privacy Act when applied to comprehensive privacy legislation covering the private sector is that if legislation does not set strict purpose and use limitations, and establish robust mechanisms for enforcement of those limitations, there will always be an incentive for companies to retain and use data beyond its initial purpose—to the point where the restriction becomes no restriction at all.

The E-Government Act, enacted in 2002, was intended to make federal agencies more accessible to the public by electronic means. The Act created an Office of Electronic Government within the Office of Management and Budget and requires that regulatory proceedings and other material appear on agency web sites. Crucially, section 208 of the Act requires agencies to perform Privacy Impact Assessments (PIAs) before procuring an information system that will process personal data or initiating a new collection of personal information.

When implemented properly, PIAs force government agencies and other institutions to carefully evaluate and publicly disclose the privacy risks of a proposed action, system, or project. An impact assessment enables the entity to identify privacy risks, to determine how and if those risks can be mitigated, and to make an informed decision whether the proposed collection or system can be justified in light of its privacy impact. An impact assessment also serves to inform the public of a data collection or system that poses a threat to privacy.

²⁷ *Id.* at § 552a(a)(7).

²⁸ Gellman, Robert, *From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974*, 23-37 (May 12, 2021), available at <https://ssrn.com/abstract=3844965>.

²⁹ *Doe v. Chao*, 540 U.S. 614 (2004).

³⁰ *FAA v. Cooper*, 566 U.S. 284 (2012).

Privacy impact assessments—or data protection impact assessments—are also required by the European Union’s General Data Protection Regulation (GDPR) for all high-risk data processing activities. Article 35 of the GDPR states:

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.³¹

However, the key to making impact assessments effective lies in enforcement. Without proper guidance and enforcement mechanisms, agencies and private companies will simply see PIAs as a box-checking exercise that must be completed for compliance rather than a substantive analysis of whether and how the entity should collect or use personal data.³²

A recent example lies in the PIA conducted by the Internal Revenue Service prior to contracting with third-party vendor ID.me for identity verification.³³ The PIA lifts language directly from ID.me’s corporate materials.³⁴ The PIA also doesn’t make mention of the one-to-many facial recognition system that ID.me has admitted to using.³⁵ In fact, despite the massive and well-known privacy and bias issues with facial recognition technology, the only facial matching technology referenced in the PIA is “comparing still ... or video ... selfies against the photo evidence uploaded by the user.”³⁶

As with the Privacy Act, courts have made it exceedingly difficult to enforce the personal data provisions of the E-Government Act through private action. In a pair of decisions from 2017 and 2019, the D.C. Circuit held that organizations and individuals cannot rely on an agency’s failure and publish a PIA to stop the agency’s unlawful processing of personal information.³⁷ As a result, there are few if any consequences for agencies that bypass the requirements of section 208.

This demonstrates just how critical it is that Congress establish a broad and express private right of action in privacy legislation. Rulings under the Privacy Act and E-Government Act have shown that without a robust private right of action, statutory rights will not be adequately enforced and privacy harms will continue undeterred. As I discuss later in my testimony, it also demonstrates the need for a federal Data Protection Agency that can serve as a

³¹ Regulation (EU) 2016/679 of the European Parliament, Article 35.

³² See Ari Ezra Waldman, *Privacy, Practice, and Performance*, California Law Review, Vol. 110, 19-21 (2021).

³³ Internal Revenue Service, *Privacy Impact Assessment: SADI CSP – ID.me* (Nov. 2021), <https://www.irs.gov/pub/irs-pia/id-me-pia.pdf> (hereinafter “IRS PIA”).

³⁴ See *Id.* at 10 and ID.me, Privacy Policy, 5, <https://www.id.me/privacy>.

³⁵ Tonya Riley, *ID.me CEO backtracks on claims company doesn’t use powerful facial recognition tech*, Cyberscoop (Jan. 26, 2022), <https://www.cyberscoop.com/id-me-ceo-backtracks-on-claims-company-doesnt-use-powerful-facial-recognition-tech/>; Ina Fried, *ID.me CEO apologizes for misstatements on IRS facial recognition*, Axios (Jan. 27, 2022), <https://www.axios.com/idme-ceo-apologizes-misstatements-irs-facial-recognition-88ce2ee2-9ae9-426c-b69e-c0b42ad82f61.html>.

³⁶ IRS PIA, *supra* note 8 at 8.

³⁷ *EPIC v. United States Dep’t of Com.*, 928 F.3d 95 (D.C. Cir. 2019); *EPIC v. Presidential Advisory Comm’n on Election Integrity*, 878 F.3d 371 (D.C. Cir. 2017).

central authority on privacy in the federal government, with the expertise necessary to guide agencies as they conduct PIAs.

B. Private Sector Data Collection and Use Governed by Sectoral Laws

There is no comprehensive law in the United States governing the collection and use of personal data. Instead, some types and uses of data are regulated by sector-specific laws such as the Health Insurance Portability and Accounting Act (HIPAA), the Fair Credit Reporting Act (FCRA), the Children’s Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), and others, while many types of data are not protected at all.³⁸ In addition to leaving huge gaps in coverage that have allowed the expansion of data collection and abuse across many different sectors, most notably online services, this also leads to confusion by the public about what types of personal data are protected and how and increased compliance costs for businesses. The US needs a comprehensive, coherent approach to privacy and data protection.

C. Comprehensive State Privacy Laws

In recent years, largely in response to Congressional inaction, some states have enacted their own privacy laws. In 2018, the California State Legislature enacted the California Consumer Privacy Act of 2018 (“CCPA”), the first comprehensive consumer privacy law enacted in the United States. The CCPA established the right of residents of California to know what personal information about them is being collected; to know whether their information is sold or disclosed and to whom; to limit the sale of personal information to others; and to access their information held by others. The CCPA gives individuals a right to delete their data and prohibits businesses from selling the personal information of CA residents under the age of 16 without their opt-in consent. The CCPA was further updated by a ballot question approved by voters in 2021, creating the California Privacy Protection Agency.

In the past year, Virginia and Colorado have also passed broad consumer privacy laws, though of at varying levels of effectiveness when it comes to protecting privacy. And this year, state legislatures in Massachusetts, Washington, Alaska, Oklahoma, New York, Ohio, Indiana, Florida, and elsewhere are considering comprehensive privacy legislation.

III. Solutions: Congress Should Enact Comprehensive Privacy Legislation and Establish a Data Protection Agency

The basic structure of information privacy law is to place responsibilities on organizations that collect personal data and to give rights to the individuals whose data is collected. This is sensible for many reasons, including the fact that it is the entity in possession of the data that controls its subsequent use and is in the best position to limit access and protect against abuse or breach. Information privacy law also promotes transparency by making data

³⁸ See Cong. Research Service, R45631, *Data Protection Law: An Overview* (2019), available at <https://crsreports.congress.gov/product/pdf/R/R45631>.

practices more open to scrutiny and encourages the development of innovative technical approaches.

EPIC, joined by ten other privacy, consumer, and civil rights groups, has set forth a framework for Congress to use when developing a privacy law that: (1) limits the collection and use of personal data; (2) prohibits discriminatory uses of data; (3) requires algorithmic fairness and accountability; (4) bans manipulative design and unfair marketing practices; (5) limits government access to personal data; (6) provides for a private right of action; (6) preserves states' rights to enact stronger provisions; and (7) establishes a federal data protection agency to enforce these new rules.³⁹ I detail each of these principles below.

A. Limit the Collection and Use of Personal Data

Federal legislation should not take a “notice and choice” approach or rely on industry self-regulation to protect data privacy. Instead, the law should place strict limits on the collection, use, storage, and transfer of personal data. Legislation should build on the U.S. Code of Fair Information Practices and OECD Privacy Guidelines, which are widely followed and form the basis of other data protection regimes. These frameworks create obligations for companies that collect personal data and establish individual data rights. Core principles include:

- Strict data collection and use limitations
- Data minimization and deletion requirements
- Transparency about business practices
- Purpose specification
- Access, correction, and deletion rights
- Data accuracy
- Confidentiality and security requirements
- Compliance and accountability

The adoption of “data minimization” techniques is essential to data protection across the board. A company implementing data minimization measures should collect only the data necessary to provide a good or service, and not more.⁴⁰ Companies complying with their data minimization requirements must also delete personal information when it is no longer needed.

The landmark privacy law passed by Congress, the Privacy Act of 1974, which applies to government agencies, requires data minimization. Each agency that collects personal data shall “maintain in its records only such information about an individual as is relevant and necessary to

³⁹ Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Justice in the United States* (2021), <https://epic.org/wp-content/uploads/2022/01/Privacy-and-Digital-Rights-For-All-Framework.pdf>.

⁴⁰ See EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (January 2022), <https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/>; see also Access Now, *Data minimization: Key to protecting privacy and reducing harm* (May 2021), <https://www.accessnow.org/data-minimization-guide/>.

accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.”⁴¹

The recently passed update to the California Consumer Privacy Act also includes provisions requiring data minimization.⁴² The European Union General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is “[a]dequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.”⁴³

Personal data that is not collected cannot be at risk of a data breach. Recognizing the need to limit private data collection, the National Telecommunications and Information Administration (“NTIA”) has identified “reasonable minimization” as a “critical Privacy Outcome.”⁴⁴

Some types of data, and some uses of data, are especially sensitive and deserve even stricter regulation. For instance, biometric and genetic data are inherently sensitive, but even information about the products people buy and the services they search for can be used to make inferences about their health, religious beliefs, economic situations, and other characteristics that are sensitive in nature. In these situations, prohibiting certain data collection and use may be necessary.

B. Prohibit Discriminatory Uses of Data

Privacy legislation should protect against discriminatory uses of data and extend civil rights protections online.⁴⁵ Processing that leads to disparate treatment or adverse disparate impacts should be prohibited. The law should also prohibit predatory data collection practices and uses that target economically disadvantaged or marginalized communities.⁴⁶

C. Require Algorithmic Fairness and Accountability

Automated systems that use artificial intelligence or other big data tools to make decisions about individuals pose significant risks to fundamental rights. Public and private actors are increasingly using AI systems to make decisions about eligibility for jobs, education, housing, parole and bail, credit, insurance, healthcare, and government services.⁴⁷ The error,

⁴¹ 5 U.S.C. § 552a (e)(1).

⁴² Cal. Civ. Code § 1798.100(c).

⁴³ Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

⁴⁴ Nat’l Telecomms. & Info. Admin., U.S. Dep’t. Commerce, *Developing the Administration’s Approach to Consumer Privacy*, Request for Comments, Docket No. 180821780-8780-01 (Oct. 11, 2018), <https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrationsapproach-to-consumer-privacy>.

⁴⁵ See Kristen Clarke and David Brody, *It’s time for an online Civil Rights Act*, The Hill (Aug. 3, 2018), <https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act>.

⁴⁶ See generally Leadership Conf. on Civil and Human Rights, *Civil Rights Principles for the Era of Big Data*, <https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/>.

⁴⁷ Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

bias, and discrimination embedded in these systems perpetuate systemic inequities,⁴⁸ yet public agencies and private companies are not currently required to evaluate the potential impacts and biases of these systems before they use them.

Indeed, many AI systems have been deployed by both government agencies and private companies with little to no oversight and with questions regarding their effectiveness.⁴⁹ A 2019 National Institute of Standards and Technology (“NIST”) study of facial recognition tools—which are typically “AI-based”⁵⁰—found that the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.⁵¹ Specifically, NIST found that “for one-to-many matching, the team saw higher rates of false positives for African American females,” a finding that is “particularly important because the consequences could include false accusations.”⁵² A separate study by Stanford University and MIT, which looked at three widely deployed commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.⁵³ A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of U.S. Congress as convicted criminals.⁵⁴

Legislation should require meaningful transparency, enable oversight of these AI systems by developing standards for and requiring independent assessments of algorithmic impact, conducting routine and randomized screening of new systems, and requiring publication of system details and audit results.⁵⁵ The law should also require a right to human review of automated decisions. Uses of AI that subvert human and civil rights should be prohibited, such as many uses in the criminal justice system, for mass surveillance, and emotion detection.

Unless express, binding limits on the use of AI are established *now*, the technology will quickly outpace our collective ability to regulate it. Congress should not make the same self-regulatory mistakes with AI that it made with data collection and use.

⁴⁸ See Richardson, Rashida, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, 36 Berkeley Tech. L.J. 3 (2022).

⁴⁹ David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* 6 (Feb. 2020) <https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf>.

⁵⁰ Nat’l Inst. Standards & Tech., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 14 (Dec. 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

⁵¹ Nat’l Inst. Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

⁵² *Id.*

⁵³ Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15 (2018), <https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/>.

⁵⁴ Russell Brandom, *Amazon’s facial recognition matched 28 members of Congress to criminal mugshots*, The Verge (July 26, 2018), <https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition>.

⁵⁵ See e.g. H.R.6580, 117th Cong. (2022) (Algorithmic Accountability Act requires transparency and accountability for automated decision making systems).

D. Ban Manipulative Design and Unfair Marketing Practices

Legislation should prohibit dark patterns designed to manipulate individuals into making choices that are in the businesses' interests rather than their own.⁵⁶ Pay-for-privacy provisions or take-it-or-leave-it terms of service, which discriminate against those with less means, should be illegal.

E. Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government is able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.⁵⁷

Federal agencies are using data collected by private companies for law enforcement, immigration, and other purposes. This undermines legal mechanisms intended to limit such government access, such as the 4th Amendment. A detailed report in *The Wall Street Journal* in early 2020 revealed that federal agencies are accessing cell phone location data without warrants or judicial oversight.⁵⁸ These agencies are engaging in warrantless location surveillance despite the Supreme Court's ruling in *Carpenter v. United States*⁵⁹ that officers must obtain a warrant in order to collect cell phone location data. The sale of location data by data brokers, which made this warrantless tracking possible, is a threat to the privacy and security of all Americans. Congress should close the loopholes that have allowed warrantless location tracking to take place.

Federal privacy legislation should require that any government collection of personal data should have a lawful basis, be performed in accordance with applicable data protection laws, be limited in time and scope to the original purpose of collection, and be subject to independent oversight. With few exceptions, it should be conducted only with the consent of those whose personal data is collected. Personal data should not be collected in bulk, from third-party data brokers without a warrant, or through warrantless surveillance. Legislation should require agencies to appoint a Chief Privacy Officer at the leadership level with the authority to oversee and address privacy issues across the agency.

⁵⁶ See generally Rohit Chopra, *Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc.*, FTC File No. 1723186 (Sep. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_r_chopra_statement.pdf. See, e.g., Complaint of EPIC, *In re In the Matter of Amazon.com, Inc.* (Feb. 23, 2021), <https://epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf>.

⁵⁷ *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

⁵⁸ Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>.

⁵⁹ 138 S. Ct. 2206 (2018).

F. Provide for a Private Right of Action

Robust enforcement is critical to effective privacy protection. The inclusion of a private right of action with statutory damages is a crucial tool to supplement government enforcement, particularly for marginalized communities. If a company violates federal privacy law, individuals and groups of individuals, or their agents, should be able to pursue a private right of action that provides meaningful redress without a showing of additional harm. While government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate. Individuals and groups of individuals who use these online services are in a good position to identify privacy issues and bring actions to vindicate their interests.

The inclusion of a private right of action is the most important tool Congress can give to Americans to protect their privacy.

Many privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. In crafting liability provisions in privacy statutes, Congress has frequently included a liquidated damages provision to avoid protracted disputes over quantifying privacy damages. This is necessary because it is often difficult to assign a specific economic value to the harm caused by a privacy violation.

For example, when Congress passed the Cable Communications Policy Act in 1984, they established privacy rights for cable subscribers and created a private right of action for recovery of actual damages not less than liquidated damages of \$100 per for violation or \$1,000, whichever is higher.⁶⁰ The Video Privacy Protection Act specifies liquidated damages of \$2,500.⁶¹ The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state court against credit reporting agencies, users of credit reports, and furnishers.⁶² In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The Drivers Privacy Protection Act similarly includes a private right of action.⁶³ The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss or up to \$500 in damages per violation.⁶⁴

The statutory damages set in privacy laws are not large in an individual case, but they can provide a powerful incentive in large cases and are necessary to ensure that privacy rights will be taken seriously and violations not tolerated. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations.

⁶⁰ 47 USC § 551(f).

⁶¹ 18 USC § 2710(c)(2).

⁶² 15 U.S.C. §§ 1681n-1681o.

⁶³ 18 U.S.C. § 2724.

⁶⁴ 47 USC § 227(c)(5).

G. Preserve States' Rights to Enact Stronger Protections

A well-established principle in the United States is that federal privacy law should operate as a floor and not a ceiling. That means that Congress often passes privacy legislation that sets a minimum standard, or “baseline,” for the country and allows individual states to develop new and innovative approaches to privacy protection. Historically, federal privacy laws have not preempted stronger state protections or enforcement efforts. Federal consumer protection and privacy laws, as a general matter, operate as regulatory baselines and do not prevent states from enacting and enforcing stronger state statutes.

The Fair Credit Reporting Act, The Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, and the Gramm-Leach-Bliley Act are just a few of the laws which allow states to craft protections that exceed federal law.

The consequences of federal preemption are potentially severe and could include both a reduction in privacy protection for many consumers, particularly as states continue to enact their own privacy laws, and also a prohibition on state legislatures addressing new challenges as they emerge. That could leave consumers and businesses exposed to increasing levels of data breach and identity theft from criminal hackers and foreign adversaries.

Today the states are on the front lines of consumer protection in the United States. They are updating privacy laws to address new challenges. They are bringing enforcement actions to safeguard American consumers. They are establishing the data protection standards that are safeguarding the personal data of Americans from attack by foreign adversaries.

It is absolutely essential to the development of privacy safeguards that Congress establish baseline standards that all states must follow, but leave states with the freedom to update their privacy laws as new technologies and business practices emerge. As Justice Brandeis famously explained, the states are the laboratories of democracy.⁶⁵ And these laboratories are all the more crucial in the area of technology policy, which is defined by persistent and rapid change.

H. Establish a U.S. Data Protection Agency

For more than two decades, EPIC has worked to support the Federal Trade Commission in its efforts to safeguard the privacy of American consumers. But it is our view that the consumer-centric, industry-by-industry approach to privacy regulation is unworkable. Congress should establish an independent Data Protection Agency in the United States to regulate, enforce, and coordinate data protection policies across all industries and governmental entities.

The United States has historically approached privacy with a consumer lens, but that view is outdated. The commercial surveillance systems that profile us and sort us into groups through a vast, opaque system of algorithms are perpetuating systemic inequities in our society.

⁶⁵ “It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory[.]” *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (Brandeis, J. dissenting).

The harms to individuals, groups of individuals, and society at large are real, and they require real solutions that do not fit neatly into the “consumer” box.

In order to move away from the commercial approach and tackle the very real threats Big Tech poses to civil rights, individual autonomy, and democracy, the United States must create a dedicated data protection agency (“DPA”). The United States is one of the few democracies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the U.S. in the 1970s. The United States was once a global leader on privacy. The Fair Credit Reporting Act, passed in 1970, was viewed at the time as the first modern privacy law—a response to the growing automation of personal data in the United States. There is an urgent need for leadership from the United States on data protection. Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges. We also now face threats from foreign adversaries that target the personal data stored in U.S. companies and U.S. government agencies. The U.S. urgently needs a Data Protection Agency.

The DPA should be dedicated to privacy and data protection, oversight, and enforcement, with the authority and resources to address emerging privacy challenges. The DPA should examine the social, ethical, and economic impacts of data processing and oversee compliance and impact-assessment obligations. The DPA should work with the FTC and Department of Justice to address competition and growing concentration in the technology sector by reviewing and issuing guidance on the privacy and data protection implications of proposed mergers. Congress should empower a DPA with adequate resources, rulemaking authority, and effective investigatory and enforcement powers.⁶⁶

Ideally, a DPA would be given the proper oversight and enforcement tools to ensure that companies innovate around and improve privacy, rather than simply pursuing penalties for privacy violations.⁶⁷ One mechanism for this has been proposed in Senator Gillibrand’s Data Protection Act⁶⁸ – the DPA could require and oversee impact assessments of high-risk data practices, such as consumer scoring or the use of or AI or biometric data. As opposed to the FTC’s unfair and deceptive acts and practices authority, which is backward looking and attempts to remedy harms that already occurred, the DPA’s ability to regulate high-risk data practices could stop privacy harms *before* they happen and help technology companies innovate around privacy.

There is broad public support for the creating of a Data Protection Agency. A recent Data for Progress poll showed that 78% of Americans across the political spectrum support

⁶⁶ See EPIC, *The U.S. Urgently Needs a Data Protection Agency*, <https://epic.org/dpa>.

⁶⁷ See Julie Cohen, *How (Not) to Write a Privacy Law*, Knight First Amendment Institute (Mar. 2021), <https://knightcolumbia.org/content/how-not-to-write-a-privacy-law> (“An essential strategy for scaling enforcement authority involves leveraging gatekeeper power to demand and guarantee adherence to the design, operational, and monitoring requirements that public oversight processes have defined.”)

⁶⁸ S. 2134, 117th Cong. § 3 (2021).

establishing a federal agency “specifically dedicated to creating and standardizing a regulatory framework aimed at protecting Americans’ data privacy.”⁶⁹

The U.S. is one of the few advanced economies in the world without a data protection agency. The consequence is that the U.S. consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber-attack by criminals and foreign adversaries. Meanwhile companies collect vast amounts of personal data about Americans without their knowledge and without any meaningful data protection standards. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security. The need for an effective, independent data protection agency has never been greater.

IV. Congress Should Enact the Online Privacy Act

Congress can address these issues and strengthen data privacy protections in the United States by taking up a bill that incorporates many, if not all, of the suggestions outlined above. The Online Privacy Act filed by Chairwoman Lofgren and Representative Eshoo is a comprehensive framework that would place strict limits on the collection and use of personal data, extend civil rights protections online, and establish strong enforcement mechanisms via a private right of action and the creation of a U.S. Data Protection Agency.⁷⁰

The Online Privacy Act would also make important updates to require the House of Representatives, Government Publishing Office, Library of Congress, and Smithsonian Institution to implement measures to prevent the disclosure of personal information by those entities and to minimize the risk of privacy harms in their operations.

One of the Online Privacy Act’s strengths lies in its enforcement mechanisms. Without strong enforcement, many businesses will simply ignore privacy laws and accept the small risk of an enforcement action as a cost of business, as we have seen in Europe and in several states. Without independent oversight, privacy law simply becomes, as Professor Ari Ezra Waldman says, “compliance, rather than a substantive, task,” or “privacy theater.”⁷¹ The inclusion of a private right of action and establishment of a Data Protection Agency avoid this fate by ensuring that the incentives to comply with privacy statutes are in place.

The Illinois Biometric Information Privacy Act (BIPA) has proven to be the most effective privacy law in the nation due to the inclusion of a private right of action.⁷² Last November, Facebook announced that it was shutting down its face recognition system and deleting more than a billion people’s facial recognition templates.⁷³ Many advocates believe

⁶⁹ Data for Progress, Poll, 10 (July 2021), https://www.filesforprogress.org/datasets/2021/7/dfp_DPA_202107_toplines.pdf.

⁷⁰ H.R. 6027, 117th Cong. (2021).

⁷¹ Ari Ezra Waldman, *Privacy Law’s False Promise*, 97 Wash. U. L. Rev. 0773, 776 (2020); Ari Ezra Waldman, How Big Tech Turns Privacy Laws Into Privacy Theater, *Forbes Future Tense* (Dec. 2, 2021), <https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html>.

⁷² Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>.

⁷³ Facebook, *An Update On Our Use of Face Recognition* (Nov 2, 2021), <https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>.

pending BIPA lawsuits against the use of facial recognition were a major factor in Facebook's decision. In 2020, Clearview AI ended all contracts with private companies and non-law enforcement entities nationwide and canceled all accounts belonging to any entity in Illinois in response to a BIPA suit it was facing.⁷⁴

In addition to its strong enforcement mechanisms, the Online Privacy Act would also add prohibitions for discriminatory processing of data, mandate data minimization, require opt-in consent for the sale of personal information, ban dark patterns, grant data subject rights to users, and impose data security requirements on covered entities. Enactment of the Online Privacy Act would help restore the current power imbalance between the companies who collect data and individuals. EPIC recommends that Congress enact the Online Privacy Act this session.

V. Conclusion

The lack of a U.S. privacy law places not only our individual autonomy, but our democracy at risk. We have seen an increased interest among federal policymakers in recent years, but now we need action. We need comprehensive privacy legislation, robust enforcement, and resources and attention dedicated to making our online world more secure and preserving the privacy and fairness of new data systems.

Thank you for the opportunity to testify today.

⁷⁴ Nick Statt, *Clearview AI to stop selling controversial facial recognition app to private companies*, The Verge (May 2020), <https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law>.

The CHAIRPERSON. Thank you very much, Ms. Fitzgerald.
We will turn now to you, Mr. Erwin, for your testimony for five minutes.

STATEMENT OF MARSHALL ERWIN

Mr. ERWIN. Thank you, Chairperson Lofgren, Ranking Member Davis, and Members of the Committee. Thank you for offering me the opportunity to testify today.

My name is Marshall Erwin. I am the Chief Security Officer at Mozilla.

Mozilla is a nonprofit organization and open-source community. Our products, including the Firefox browser, are used by hundreds of millions of people around the world. Mozilla is constantly investing in security and privacy and advancing movements to build a healthier internet.

Now, in our view, privacy online is a mess today. Consumers are constantly under attack. They are stuck in a vicious cycle in which their data is collected without their knowledge or understanding, then shared to build profiles about them. That data is then used to target and manipulate them in ways that can be actively harmful.

Today I am going to talk about what Mozilla is doing to address this problem and then what we think Congress needs to do.

In the Firefox browser there have been two focus areas for us.

The first is that we have been driving major initiatives, such as the standardization of TLS 1.3 or founding Let's Encrypt, a free nonprofit certificate authority. This has resulted in an increase in encrypted web traffic up to almost 85 or 95 percent from below fifty percent a few years ago.

What this is doing is protecting your browsing activity and your information from attackers in the middle of a network who would otherwise collect that information to use it to build a profile about you.

The second big area of focus for us has been on eliminating what we call cross-site tracking. These are parties following you around from the website to website that you visit, again collecting your information about your browsing activity and then building that profile about you.

In 2019, we turned on what we called Enhanced Tracking Protection in the browser, turned that on by default because we believe the onus shouldn't be on consumers to protect themselves from opaque risks they can't see or understand.

So that is just a little bit of what we have been doing to try to address this problem. I want to talk a little bit about what we think Congress needs to do, first focusing on baseline Federal privacy legislation, and then talk a little bit about transparency into online harms.

First, in our view, technical privacy protections from companies and baseline regulations are complementary and necessary. Neither alone are sufficient. The internet was not designed with privacy and security in mind, which is why technical solutions like the ones that we offer are necessary to create a less permissive environment overall.

At the same time, we can't solve every privacy problem with a technical fix. There is an essential role for regulation here as well.

To give you just one example, we know that dark patterns are pervasive across the software and applications that people use. Unfortunately, there is little that a browser can do when a person visits a website directly and then is deceived into handing over their information without proper consent or understanding.

And this is where law plus a robust enforcement regime must step in. That is why provisions like the one in the Online Privacy Act, which would prohibit dark patterns, are so critical.

More generally, Mozilla supports privacy and data protection laws around the world, including in the United States. The U.S. must enact baseline privacy protections to ensure that the public and private actors treat consumers fairly. We need clear rules of the road for entities using personal data, strong privacy rights for people who are interacting with those entities, and effective authorities, agencies with the authority to take enforcement action.

Second, it is important to complement Federal privacy legislation with solutions that provide direct transparency and accountability into online harms.

Many of the harms that we see today are a direct result of the pervasive data collection happening. We know from recent whistleblower disclosures things like recommendation systems and targeting systems can have pernicious effects if abused.

These systems are really powered by people's data. It is easier to discriminate against people, manipulate people, or deceive people if you know more about them. Therefore privacy and some of these online harms are really inherently linked.

The problem is that this harm is mostly hidden from the public and from regulators. That is why we have called for things like an establishment of a safe harbor to protect researchers doing investigations into the activities of major online platforms.

This would protect research into the public interest and help us better understand the harm happening on these platforms. There is a real public benefit that can be had here by such a safe harbor.

Similarly, we have advocated for more robust disclosure regimes governing online ads. We have been leading the push for full ad disclosure in the European Union. We are encouraged by recent proposals in Congress that would require disclosure of ads for public benefit and understanding.

These approaches would provide transparency into the opaque world of online advertising. It is necessary, and we think it could be done without creating privacy risks.

In conclusion, at Mozilla we seek to advance privacy technology and to ensure that privacy considerations are at the forefront of policymakers' minds in considering how to protect consumers and grow the economy.

We appreciate the Committee's focus on these issues and look forward to the discussion.

[The statement of Mr. Erwin follows:]



**Written Statement of Marshall Erwin, Chief Security Officer
Mozilla**

**Before the Committee on House Administration
United States House of Representatives**

“Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors”

February 16, 2022

Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you for holding this hearing today on such an important issue, and for the opportunity to testify.

I'm Marshall Erwin, Chief Security Officer at Mozilla.

Our Public Mission and Incentives

Mozilla is a unique public benefit organization and open source community formed as a non-profit foundation. We build the open-source Firefox web browser, Mozilla VPN, and the Pocket “read-it-later” application. These products are used by hundreds of millions of individuals around the world. As a mission-driven technology company and a non-profit foundation, we are dedicated to putting people in control of their online experience, and creating an internet that is open and accessible to all.

To fulfill this mission, we are constantly investing in the security of our products, the privacy of our users and in advancing the movement to build a healthier internet. Mozilla has influenced major companies to adopt better privacy practices such as browser anti-tracking measures and empowered people directly with tools to better understand and block third party data collection. For Mozilla, privacy is not optional. It is an integral aspect of our founding principles, which state that individuals' security and privacy on the internet are fundamental and must not be treated as optional.

Mozilla's Meaningful Protections by Default and Design

We have worked hard to make Mozilla's vision for privacy and security a reality in the products we build and the technologies we develop. We do this by leading and participating in the creation of web standards that make the internet more secure and more protective of privacy, and by pioneering the product-level implementation of privacy and security-enhancing browser technologies through Firefox. These open innovations are available to the wider internet: other organizations, internet applications, and consumers.

For example, we have made online commerce and navigation safe through protocols and initiatives like TLS 1.3 and Let's Encrypt. TLS 1.3 is the protocol that powers every secure transaction on the internet. Let's Encrypt is a major internet security success story; because of its creation, 85% of online traffic is now encrypted with HTTPS (signaled by a green padlock on many web browsers), compared to less than 30% in 2014.

We have always put privacy first in our own products and features.

- In 2019 we enabled **Enhanced Tracking Protection**¹ by default in Firefox, protecting our people from cross-site tracking. While anti-tracking features had been available for many years in Firefox, we turned this feature on by default because we believe² that the onus should not be on consumers to protect themselves from sophisticated privacy risks they do not understand.
- Last year, we introduced one of our strongest privacy protections to date, **Total Cookie Protection**,³ to provide additional protections from cross-site tracking.
- Mozilla has also been instrumental in the technological development and product roll-out of technologies to encrypt web traffic. This includes most recently our work on **DNS over HTTPS**⁴ - or DoH - the protocol that encrypts domain name look-ups and closes one of the last great security vulnerabilities in the internet architecture.

¹ Dave Camp, "Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise," Mozilla dist://ed (June 4, 2019), at <https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/>

² Steven Englehardt, "Why we need better tracking protection," Mozilla Security Blog (Sept. 5, 2018), at <https://blog.mozilla.org/security/2018/09/05/why-we-need-better-tracking-protection/>

³ Selena Deckelmann, "Latest Firefox release includes Multiple Picture-in-Picture and Total Cookie Protection," Mozilla dist://ed (Feb. 23, 2021), at <https://blog.mozilla.org/en/products/firefox/latest-firefox-release-includes-multiple-picture-in-picture-and-total-cookie-protection/>

⁴ Patrick McManus, "Improving DNS Privacy in Firefox," Firefox Nightly News (June 1, 2018), at <https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/>

- Our **VPN** (Virtual Private Network)⁵ helps people create a secure, private connection to the internet.
- And our end-to-end encrypted **Firefox Sync**⁶ service by default protects all your synced data so Mozilla can't read it.

We also support practical solutions to help companies have a healthier relationship with data, through our Lean Data Practices (LDP) framework and trainings.⁷ LDP helps other organizations to reduce the amount of user data that is initially collected and focuses on only collecting essential data to lower risk and promote trust with users. We have published this framework under an open license, and have worked with organizations around the world to educate other businesses on the benefits of such an approach. We have learned through LDP workshops with public sector participants that the absence of a uniform data protection law causes challenges to minimize, delete, and limit the sharing of data today. Especially at the local level, there may also be a lack of resources to better secure data or explain to constituents how it is used and shared.

Addressing the Systemic Privacy Problem Through Legislation

While we play an important role in keeping people secure and protecting privacy on the internet, we nonetheless recognize that the lack of privacy online today is a systemic problem. We need structural change to protect data and empower people. We therefore believe that law and regulation have an essential role to play in creating a healthier internet. Relying on the voluntary adoption of protocols and practices like the ones we have designed is an incomplete solution.

In our view, technical privacy protections by companies and privacy regulation are complementary and necessary. Neither alone is sufficient. The internet was not originally designed with privacy and security in mind, which is why technical solutions are necessary to create a less permissive environment that is more protective of people. But we cannot solve every privacy problem with a technical fix.

For example, we know that dark patterns are pervasive across the online applications that people engage with daily. Unfortunately, there is little any browser can do when a person visits a website directly and is deceived by the website into handing over and sharing their data without meaningful consent. This is where law, plus a robust enforcement regime, must step in. That is why provisions such as the one in the *Online Privacy Act* that prohibit dark patterns are so critical.

⁵ Mozilla VPN, at <https://www.mozilla.org/en-US/products/vpn/more/what-is-a-vpn/>

⁶ Firefox Sync, at <https://www.mozilla.org/en-US/firefox/sync/>

⁷ Mozilla Lean Data Practices, at <https://www.mozilla.org/en-US/about/policy/lean-data/>

Another example is what we call browser fingerprinting, which is a technique used to track consumers by constructing an identifier from the characteristics of their browser. Fingerprinting is opaque to users and would fail to satisfy many user privacy rights regimes. Mozilla attempts to block fingerprinting in Firefox, but we recognize that we will not be able to defeat all fingerprinting activities, no matter how we change our browser. In areas like these, technical solutions will not be enough.

This is why Mozilla strongly supports privacy and data protection laws around the world, including in the US. The US should enact baseline federal privacy protections, to ensure public and private actors treat consumers fairly. We need clear rules of the road for entities using personal data, strong rights for people who interact with those entities, and effective authority for the Federal Trade Commission (FTC) to make and enforce these rules as technologies evolve. Ultimately, privacy, security, and consumer data protection are best-served when policy is based upon a comprehensive framework of protections.

Greater Transparency into Hidden Harms

Many of the harms we see on the internet today are in part a result of pervasive data collection and underlying privacy risk. Targeting and personalization systems generate real value for consumers. But, as we have learned from recent whistleblower disclosures, these systems also can be abused, resulting in real world harm to individuals and communities. They are powered by people's data. Indeed, the more you know about someone, the easier it will be to deceive, or peddle disinformation, or discriminate against them.

The world has now had a few years of experience with global and state laws covering baseline data and security requirements. Unfortunately, there remains a looming gap, which is that we lack sufficient insights into how people experience online discrimination and harm when their data is collected, used and shared without meaningful awareness or consent. This includes what ads are presented to you and why, and what content is recommended to you and why. To address this, we need complementary regulatory solutions to federal privacy legislation that would provide greater levels of transparency into the ecosystem impact of our online data.

At Mozilla, we support solutions that will provide greater transparency into online discrimination and harms that today are hidden from the public and from regulators. Accordingly, we have called for establishing a safe harbor allowing researchers,

journalists, and others to access relevant datasets, free from threats of legal action. Such a safe harbor should protect research in the public interest as long as researchers handle data responsibly and adhere to professional and ethical standards. We know there is enormous value this can provide to the public. Mozilla has one of the earliest Bug Bounty programs in software. We make clear that we will not threaten or bring any legal action against anyone who makes a good faith effort to comply with our vulnerability notification policy because this encourages security researchers to investigate and disclose security issues. Their research helps make the internet a safer place.

Similarly, we advocate for a more robust disclosure regime governing the ads people see online. We have been leading the push for full ad disclosure in the European Union's Digital Services Act and we are encouraged by recent proposals in Congress that would require disclosure of ads for public benefit and understanding. These approaches would bring transparency into the opaque world of online advertising and can be done in ways that do not pose privacy risk to users.

Structural Solutions Should be Used to Limit First Party Data Use

Federal privacy law, while essential, should also be bolstered by regulation and enforcement to foster stronger consumer protection and competition. The most dominant technology companies today are the largest third-party trackers on the internet. At the same time, the same companies also have extensive first party relationships with consumers and have benefited the most from the absence of oversight to protect consumers.

We support efforts by regulators to tackle this problem through interventions governing how data can be shared and used within the holding structures of large platforms. For example, we strongly support Google's recent commitments to UK regulators to foreclose the use of data from Android, Chrome browsing history and sync data, Google Analytics, and Customer Matching for targeting after implementation of Chrome Privacy Sandbox proposals. This is a positive direction for the evolution of a more private and secure internet that will benefit consumers around the world. Indeed, all dominant platforms should embrace commitments like this and start practicing them immediately, beyond just advertising or browser technologies, to ensure a fairer and more interoperable internet for everyone.

At the same time, it is important that competition concerns not be a pretext to prevent better privacy for everyone. Many parties, large and small, have built their business

models to depend on extensive user tracking. Many third-party advertising companies that depend on ubiquitous user tracking seek to prevent privacy innovation. Closing privacy gaps necessarily means denying data to these parties. That is a good thing. Consumer welfare is at the heart of both competition and privacy enforcement. Focusing on consumers and their needs will ensure regulation doesn't inadvertently freeze the evolution of internet technologies that can offer consumers advances in privacy and security.

Conclusion

At Mozilla, we seek to advance a favorable environment for privacy-enhancing technologies, and to ensure that privacy considerations are front and center of policymakers' minds when considering how to protect consumers and grow our economy.

We believe through our product and policy work we can help address the data privacy gaps that exist today, impacting consumers, companies, and the public sector alike. Despite being a powerhouse of technology innovation for years, the United States is behind globally when it comes to recognizing consumer privacy and protecting people from indiscriminate data collection and use. We appreciate the Committee's focus on this vital issue and look forward to further discussions with Congress. Thank you.

The CHAIRPERSON. Thank you, Mr. Erwin.
And now we turn to our last but certainly not our least witness, Mr. Castro, for your testimony for five minutes.

STATEMENT OF DANIEL CASTRO

Mr. CASTRO. Thank you. Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, I appreciate the invitation to speak with you today.

U.S. data privacy is at a crossroads. Many consumers are justifiably frustrated by the frequency with which they learn about new data breaches and the seeming lack of accountability for those who misuse their personal information.

At the same time, many firms are overwhelmed by a tsunami of new data-protection obligations and growing restrictions on how they can use personal information for legitimate business purposes. All are often confused by the multitude of ever-changing laws and regulations.

Three States, California, Virginia, and Colorado have passed comprehensive data privacy legislation, and many other States are considering it. Over the past three years, 34 State legislatures have introduced a total of 72 bills and more are coming.

These new State privacy laws can impose significant costs on businesses, both direct compliance costs and decreases in productivity, and undermine their ability to responsibly use data to innovate and deliver value to consumers.

Moreover, these laws create high costs, not just for in-State businesses, but also for out-of-State businesses that can find themselves subject to multiple and duplicative laws. For example, California's recently enacted privacy law will likely cost \$78 billion annually, with California's economy bearing \$46 billion and the rest of the U.S. economy bearing the other \$32 billion.

In the absence of Federal data privacy legislation, the growing patchwork of State privacy laws could impose out-of-State costs between \$98 billion and \$112 billion annually. Over a ten-year period, the costs would exceed \$1 trillion. The burden on small businesses would be substantial, with U.S. small businesses bearing \$20 billion to \$23 billion annually.

The United States needs a new Federal data privacy law, but it should not back away from the light-touch approach it has historically taken to regulating the digital economy. Instead, it should focus on the following goals.

First, data privacy legislation should establish basic consumer data rights. For example, Congress should give individuals the right to know how organizations collect and use their personal data or when their information has been part of a data breach.

Congress should also give consumers the right to access, port, delete, and rectify their sensitive data in certain contexts. For example, consumers should have a right to obtain a copy of their health or financial data and move it to a competing service.

Second, lawmakers should establish uniform privacy rules for the entire Nation by preempting State and local privacy laws. Consumers should have the same protections regardless of where they live, and companies should not be faced with 50 different sets of laws and regulations.

A patchwork of State laws, with varying definitions and standards, creates a complex regulatory minefield for businesses to navigate, especially if potential violations risk costly litigation.

Third, Congress should ensure there is robust and reliable enforcement of Federal privacy law. Congress should not create a private right of action, and instead rely on Federal and State regulators to hold organizations accountable.

Illinois, which has a private right of action for its biometrics law, has seen hundreds of lawsuits in the past two years even when there has been no consumer harm.

And, to avoid unnecessary litigation, businesses should have a reasonable period to address a violation without penalty in cases with no demonstrable consumer harm, such as a sixty-day notice-and-cure period.

Fourth, Congress should set a goal of repealing and replacing potentially duplicative or contradictory Federal privacy laws. The U.S. Code right now is littered with privacy statutes, from major sections on health and financial data to narrow ones on video rental histories, and each one has its own set of definitions and rules to comply with.

Finally, Federal data privacy legislation should minimize the impact on innovation. To that end, Congress should not include data-minimization, purpose-specification, or privacy-by-design requirements because these provisions can reduce access to data, limit data sharing, and constrain its use, thereby limiting beneficial innovation.

Congress has the benefit of hindsight to avoid some of the problems found in other data privacy laws, particularly Europe's GDPR, or General Data Protection Regulation. The GDPR has imposed massive compliance costs on businesses, not only in the EU, but around the world. For example, Fortune 500 companies have spent nearly \$8 billion to comply with the GDPR.

Unfortunately, the GDPR has not delivered on many of its goals. For example, the EU's own surveys show that the law has had virtually no impact on consumer trust in the internet. A majority of companies also report that some of the most expensive requirements, like appointing a data protection officer, serve no valuable business function.

Policymakers should also be aware of the unintended consequences of poorly crafted legislation, such as not considering the implications of a law on emerging technologies like artificial intelligence and blockchain.

Finally, Congress should note that the primary purpose of the GDPR was to harmonize data protection laws across EU member states. Ironically, as States pursue their own laws, they are creating the exact type of fragmentation in the U.S. that the EU created the GDPR to solve.

So, therefore, it is essential for Congress to act swiftly to pass comprehensive privacy legislation that preempts State laws, streamlines regulation, establishes basic consumer data rights, and minimizes the impact on innovation.

Again, thank you for the opportunity to be here today. I look forward to any questions.

[The statement of Mr. Castro follows:]



**Testimony of
Daniel Castro
Vice President
Information Technology and Innovation Foundation**

**Before the
Committee on House Administration**

**Hearing on
“Big Data: Privacy Risks and Needed Reforms
in the Public and Private Sectors”**

February 16, 2022
1310 Longworth House Office Building
Washington, DC

Chairperson Lofgren, Ranking Member Davis, and members of the committee, thank you for the opportunity to appear before you to discuss privacy risks and potential reforms.

I am the vice president of the Information Technology and Innovation Foundation (ITIF). ITIF is a nonprofit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity. I am also the director of the Center for Data Innovation, a research institute at ITIF focusing on the intersection of data, technology, and public policy.

In my testimony today, I would like to provide an overview of why Congress should pass data-privacy legislation, what that legislation should look like, and how the United States can avoid the mistakes made in the EU's General Data Protection Regulation (GDPR) and other data-privacy laws.

WHY CONGRESS SHOULD PASS DATA-PRIVACY LEGISLATION

U.S. data privacy is at a crossroads. Many consumers are justifiably frustrated by the frequency with which they learn about new data breaches and the seeming lack of accountability for those who misuse personal information. At the same time, many businesses are overwhelmed by the tsunami of new data-protection obligations they face and the growing restrictions on how they can use personal information. And all are confused by the multitude of ever-changing laws and regulations.

These conditions have created a groundswell of support for new data-protection laws. Over the past few years, federal and state lawmakers have proposed various privacy laws to regulate the collection and use of personal data. Three states—California, Virginia, and Colorado—have passed comprehensive data-privacy legislation that gives consumers in those states new rights regarding the collection of their personal information and imposes new obligations on businesses. Many other states have considered enacting similar privacy laws. Between 2018 and 2021, 34 state legislatures have introduced a total of 72 bills, which have advanced to various stages of the legislative process.

These new state privacy laws can create confusion for consumers and impose significant costs on businesses—both direct compliance costs and decreases in productivity—and undermine their ability to responsibly use data to innovate and deliver value to consumers. Moreover, these laws create high costs not just for in-state businesses, but also for out-of-state businesses that can find themselves subject to multiple and duplicative rules. For example, California's recently enacted privacy law will likely cost \$78 billion annually, with California's economy bearing \$46 billion and the rest of the U.S. economy bearing the other \$32 billion. California small businesses will bear \$9 billion of in-state costs, while out-of-state small businesses face \$6 billion of costs.¹

In the absence of federal data-privacy legislation, the growing patchwork of state privacy laws could impose out-of-state costs between \$98 billion and \$112 billion annually.² Over a 10-year period, these costs would exceed \$1 trillion. The burden on small businesses would be substantial, with U.S. small businesses bearing \$20 billion to \$23 billion annually.³

WHAT FEDERAL DATA-PRIVACY LEGISLATION SHOULD ACCOMPLISH

Although the United States needs a federal data privacy law, it should not back away from the light-touch approach it has historically taken to regulating the digital economy. Instead of pursuing a broad, European-style data-privacy law that would impose significant costs on the U.S. economy, Congress should craft targeted legislation that creates a national privacy framework that establishes basic consumer data rights, preempts state laws, ensures reliable enforcement, streamlines regulation, and minimizes the impact on innovation. Such legislation should address concrete privacy harms, not hypothetical ones, and improve transparency so consumers better understand how businesses use their data. It should strengthen oversight and enforcement through the FTC and avoid unnecessary litigation costs by not including a private right of action. It should also protect and promote innovation by minimizing compliance costs and restrictions on data use, such as by avoiding data minimization and purpose specification requirements.

First, federal data privacy legislation should establish basic consumer data rights. Lawmakers should not treat all data the same, but instead create rules that are tailored for different types of data and the contexts in which they are collected. To that end, privacy legislation should make a distinction between sensitive and non-sensitive personal data, because sensitive personal data—such as medical or location information—presents higher risk to people if it is made public.

The idea is to create a sliding scale where the most sensitive personal data collected in the most sensitive contexts (e.g., a doctor's office collecting a patient's health data) is subject to the strictest rules and penalties to prevent misuse, and non-sensitive data collected in a non-sensitive context (e.g., a grocery store tracking what kind of cereal shoppers buy) would be subject to the fewest requirements. With a tiered set of rules like this, consumers would receive stronger privacy protections where it matters most, and businesses could avoid undue compliance burdens.

Congress should give individuals the right to know how organizations collect and use any of their personal data or when their information has been part of a data breach, but consider limiting other rights, such as the right to access, port, delete, or rectify their data, to only sensitive data in certain contexts. For example, consumers should have a right to obtain a copy of their health or financial data and move it to a competing service.⁴ Similarly, Congress should establish user consent requirements for data collection, sharing, and use based on a similar sliding scale. For example, health apps should need to obtain permission from consumers before sharing their sensitive health information with third-party researchers, but florists should be able to send their loyal customers a coupon unless they opt out.

Second, lawmakers should establish uniform privacy rules for the entire nation by preempting state and local privacy laws. Consumers should have the same protections regardless of where they live, and companies should not be faced with 50 different sets of laws and regulations. A patchwork of state laws with varying definitions and standards creates a complex regulatory minefield for businesses to navigate, especially if potential violations risk costly litigation. The goal of Congress should be to minimize unnecessary compliance costs for businesses so that they can concentrate their resources not on hiring more privacy lawyers to protect them from potential fines for non-compliance but on investments that will lead to more secure and privacy-preserving products and services.

Third, Congress should ensure there is robust and reliable enforcement of federal privacy law. Congress should give the Federal Trade Commission (FTC) sufficient resources and authority to fine organizations that impose actual harms on individuals through data misuse. Congress should also give the FTC authority to conduct limited rulemakings for data privacy for issues like deciding the right way for companies to disclose their data handling practices. However, the legislation should be very specific in how the FTC can exercise its authority to ensure regulators do not impose heavy-handed rules about the design of user experiences for websites and mobile apps (i.e., “dark patterns”).

Enforcement is important because it enables regulators to have oversight over organizations while ensuring they are held accountable when they do not follow the rules. However, Congress should be careful not to create duplicative or inconsistent enforcement mechanisms that would impose high costs for organizations. Indeed, if both regulators and private parties can pursue cases for identical reasons, firms can be tied up in lawsuits for years and pay hefty fees for each incident. To that end, Congress should not allow a private right of action, and instead rely on federal and state regulators to hold organizations accountable. In addition, organizations should only be subject to significant fines if they have caused actual economic harm. And to avoid unnecessary litigation, federal privacy legislation should allow for a reasonable period of time for organizations to address a violation without penalty in cases with no demonstrable consumer harm (e.g., establish a 60-day notice and cure period).

Fourth, Congress should set a goal of repealing and replacing potentially duplicative or contradictory federal privacy laws. The U.S. code is littered with privacy statutes—from major sections on health and financial data to narrow ones on video rental histories—and each one has its own set of definitions and rules to comply with.⁵ Congress should create a roadmap to repeal and replace all of them with a single, comprehensive data privacy law. Such a major overhaul may sound daunting, but the alternative—adding another layer to the pile—will undermine the purpose of new legislation.

Finally, federal data privacy legislation should minimize the impact on innovation. To that end, Congress should not include data-minimization requirements, purpose-specification requirements, or privacy-by-design requirements because these provisions can reduce access to data, limit data sharing, and constrain its use, thereby limiting innovation. For example, purpose-specification requirements obligate organizations to disclose to users the purposes for which they are collecting information and then not use this collected data for any other reasons. This requirement limits organizations from reusing data for new purposes, which limits innovation. Purpose-specification requirements also limit organizations that may already be collecting useful data from extracting value from that information, such as by applying data analytics. Neither should Congress impose limitations on data retention or automated decision-making, as these provisions would similarly restrict organizations from efficiently using data.

HOW TO AVOID THE MISTAKES OF THE GDPR AND OTHER PRIVACY LAWS

Consumers and businesses would clearly benefit from a federal data-privacy law, but imposing a European-style law on American businesses recovering from a global pandemic would slow economic recovery by saddling companies with unnecessary red tape while limiting beneficial uses of data. Indeed, Congress can

benefit from hindsight by looking back at some of the negative consequences of GDPR, which went into effect in May 2018, and other privacy laws.

Avoid Excessive Compliance Costs

Congress should avoid enacting a privacy law that imposes excessive compliance costs. The GDPR has imposed massive compliance costs on businesses, not only in the EU but around the world. The Global Fortune 500 has spent an estimated €7 billion in compliance costs for GDPR.⁶ In one survey, over 40 percent of companies, including U.S. firms with a data presence in the EU, had spent \$10.1 million in compliance efforts.⁷ In another, companies reported spending an average of \$1.3 million in 2017 on GDPR compliance and were expected to spend an additional \$1.8 million in 2018.⁸

Understand That More Regulation Does Not Always Benefit Consumers

Although some tout the GDPR as the gold standard for consumer protection, it has not always lived up to its reputation. For example, the law has had virtually no impact on consumer trust in the digital economy: Six months after it went into effect, consumer trust in the Internet was at its lowest in a decade in the EU.⁹ A year after the law went into effect, nearly two-thirds of Europeans (63 percent) had never heard of the GDPR (31 percent) or did not know exactly what it is (32 percent).¹⁰ The European Commission has found that “at a country level there is no consistent relationship between awareness of GDPR and the level of control respondents feel they have over the personal information they post online.”¹¹ Moreover, many of these costs appear to do nothing to enhance consumer privacy. According to an October 2018 survey, a majority of companies that have appointed a data protection officer (52 percent) say they established one for compliance reasons only, and that the role does not serve a valuable business function.¹²

Ensure Sufficient Resources for Regulators

Congress should ensure regulators have sufficient resources to handle any new obligations. The GDPR caught many regulators flat-footed. For example, the UK’s Information Commissioner’s Office (ICO) said its staff and services were overwhelmed by companies “over-reporting” potential data breaches because of concerns over high penalties if they failed to notify the data protection authority (DPA) within the GDPR’s tight 72-hour reporting deadlines.¹³ Similarly, a spokesman of CNIL, the French DPA, declared that “the resources of the CNIL are insufficient” to enforce the GDPR.¹⁴

Beware of Unintended Consequences

Perhaps the most important lesson for policymakers from the GDPR is to beware of the unintended consequences of poorly crafted data-privacy legislation. For example, because the drafters of the GDPR never fully considered the implications of the law on emerging technologies like artificial intelligence and blockchain, they included a number of provisions that make it difficult, and sometimes virtually impossible, for businesses to use them.¹⁵

Some of the most significant unintended consequences are economic. For example, the GDPR has negatively impacted venture funding for EU tech firms. Between May 2018 and April 2019, the overall venture funding for EU tech firms decreased by \$14.1 million per month per member state.¹⁶ The decrease in investments for

young ventures caused by the GDPR could result in a yearly loss of up to approximately 30,000 jobs in the EU.¹⁷ Or consider that 55 percent of the 539 mergers and acquisitions (M&A) professionals from Europe, Africa, and the Middle East surveyed in July 2018 declared having worked on transactions that did not go through due to concerns about companies' compliance with the GDPR.¹⁸

Some of these unintended consequences are also felt directly by consumers. Two months after the GDPR went into effect, a third of the largest U.S. news websites had to block access to the EU as they had not yet managed to comply.¹⁹ Almost a year later, in March 2019, 1,129 U.S. news websites still remain blocked, including Pulitzer prize-winning publishers like the *Chicago Tribune*.²⁰ Companies have also interrupted some of their online services in the EU because of concerns over complying with the GDPR, including Czech platform Seznam, which had to shut down its student social network, and online gaming company Gravity Interactive, which blocked European users from accessing its games and services.²¹

Policymakers should also consider how individuals might misuse new privacy laws. For example, one of Finland's highest courts ruled in August 2018 that the GDPR's "right to be forgotten" could give a convicted murderer the right to have publicly available information about his crime removed from Google search listings, superseding the country's and the EU's own laws protecting freedom of speech and the right to access information.²² Online tools have also been created to weaponize the GDPR against companies, such as overloading businesses with GDPR-authorized data requests that must be addressed within 30 days with the stated purpose to "waste their time."²³

The COVID-19 pandemic also offered a lesson on the unintended consequences of the GDPR. At the beginning of the pandemic, Italy, one of the countries in Europe hit hardest by COVID-19, found that the GDPR prevented businesses from taking basic steps to track and trace potential infections, such as employers recording body temperatures to ensure compliance with safety protocols for essential workers. Similarly, the French data regulators noted that the GDPR prevented employers from using thermal cameras to automatically check temperatures of their workers.²⁴

As the pandemic progressed, it became clear that the GDPR had also become a barrier to biomedical research—the very research necessary to save lives and reopen the economy. The GDPR creates significant challenges for research organizations in the EU sharing data with researchers located in most countries outside the EU. Indeed, a team of researchers from the United States, Canada, and the EU published an article in *Science* arguing that "the GDPR's limitation on data transfers will hamper science globally in general and biomedical science in particular."²⁵

Prevent Costly Lawsuits

In addition to the GDPR, Congress can learn from some of the state privacy laws. In particular, the Illinois Biometric Information Privacy Act (BIPA) demonstrates the risk of costly litigation when privacy laws create a privacy right of action. BIPA was designed to regulate the collection of biometric data by companies operating in Illinois or whose products reached consumers in that state. Although BIPA passed into law in 2008, it was not until 2019 that the Illinois Supreme Court held that individuals are not required to show actual harm to bring consumer class action lawsuits and employer lawsuits. This ruling means that individuals can file

lawsuits even when there has only been a technical violation of the law.²⁶ Since then, the number of BIPA lawsuits has skyrocketed—In 2019, there were around 300 lawsuits, and the number of cases referencing BIPA doubled in 2020.

California offers another example of this dynamic. The California Consumer Privacy Act of 2018 (CCPA) applies to firms that do business in California, including those without a physical presence. The law allows consumers to seek damages when their personal information is inappropriately accessed or disclosed because a business failed to maintain reasonable security procedures. Since California enacted the law in 2020, plaintiffs have filed approximately 195 lawsuits against businesses in many different industries.²⁷

Lawsuits can lead to major settlements, thereby threatening the viability of smaller businesses and imposing steep costs on larger ones. Even if a business can prevail in a lawsuit, the costs of the lawsuit are often significant, especially in state courts that are often more favorable for plaintiffs in class action litigation compared with federal courts and allow for expensive discovery processes, such as requesting documents and witness interviews, that can drive up the costs of litigation very quickly.

CONCLUSION

It is essential for Congress to craft well-designed federal data privacy legislation. Poorly designed data privacy laws can impose a substantial toll on the economy through both direct compliance costs and indirect costs from lower productivity and constraints on innovation. Unnecessarily restrictive rules for the digital economy reduce innovation in ways that harm both businesses and consumers. By raising compliance costs, increasing legal risks, and reducing the effectiveness of online business models, poorly drafted rules can lead to a reduction in the supply of, and demand for, digital services.

It is equally important for Congress to proceed swiftly with new data privacy legislation. In the absence of a new law, states will continue to enact their own competing, and potentially contradictory, data privacy laws. One of the primary purposes of the GDPR was to harmonize data protection laws across EU member states, and ironically, by pushing for new laws modeled after the GDPR, state legislatures are creating the exact type of fragmentation in the United States that the EU created the GDPR to solve.

To avoid conflicting laws and unnecessary costs, Congress should act swiftly to pass comprehensive privacy legislation that preempts state laws, streamlines regulation, establishes basic consumer data rights, and minimizes the impact on innovation (e.g., by avoiding requirements for data minimization, universal opt-in, purpose specification, limitations on data retention, or privacy-by-design). This legislation should not include a private right of action and instead rely on federal and state regulators for enforcement. Establishing a comprehensive federal privacy law would also simplify compliance for businesses, especially small businesses working across multiple U.S. jurisdictions, as well as help consumers better understand their privacy rights and avoid the confusion resulting from a patchwork of state laws.

Thank you again for this opportunity to appear before you today.

REFERENCES

-
- ¹ Daniel Castro, Luke Dascoli, and Gillian Diebold, “The Looming Cost of a Patchwork of State Privacy Laws,” (Information Technology and Innovation Foundation, January 2022), <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws>.
- ² Ibid.
- ³ Ibid.
- ⁴ Daniel Castro, “Improving Consumer Welfare with Data Portability,” (Center for Data Innovation, November 2021), <https://www2.datainnovation.org/2021-data-portability.pdf>.
- ⁵ For example, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Family Educational Rights and Privacy Act (FERPA) apply to data in the health, financial, and educational sectors, respectively.
- ⁶ Forbes, “The GDPR Racket: Who’s Making Money From This \$9bn Business Shakedown” (May 2, 2018), <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#38765ac234a2>.
- ⁷ PriceWaterhouseCoopers, “Pulse Survey: GDPR budgets top \$10 million for 40% of surveyed companies” (December 9, 2017), <https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html>.
- ⁸ IAPP and Ernst & Young, “Annual Governance Report 2018” (IAPP and Ernst & Young, 2018), <https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/>.
- ⁹ Daniel Castro and Eline Chivot, “The GDPR Was Supposed to Boost Consumer Trust. Has it Succeeded?” European Views, June 6, 2019, <https://www.european-views.com/2019/06/the-gdpr-was-supposed-to-boost-consumer-trust-has-it-succeeded/>.
- ¹⁰ European Commission, “Special Eurobarometer 487a, The General Data Protection Regulation” (June 2019), <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222>.
- ¹¹ Ibid.
- ¹² IAPP and Ernst & Young, “Annual Governance Report 2018” (IAPP and Ernst & Young, 2018), <https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/>.
- ¹³ Information Commissioner’s Office, “CBI Cyber Security: Business Insight Conference. ICO Deputy Commissioner (Operations) James Dipple-Johnstone – speech to the CBI Cyber Security: Business Insight Conference” (ICO, September 12, 2018), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/cbi-cyber-security-business-insight-conference/>.
- ¹⁴ Wall Street Journal, “European Privacy Regulators Find Their Workload Expands Along With Authority” (April 12, 2019), <https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402>.
- ¹⁵ Eline Chivot and Daniel Castro, “The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy,” Center for Data Innovation, May 13, 2019, <https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/>.
- ¹⁶ Jian Jia, Ginger Zhe Jin, and Liad Wagman, “The Short-Run Effects of GDPR on Technology Venture Investment” (May 31, 2019), <http://dx.doi.org/10.2139/ssrn.3278912>.
- ¹⁷ Jian Jia, Ginger Zhe Jin, and Liad Wagman, “The short-run effects of GDPR on technology venture investment” (VOX CEPR Policy Portal, January 7, 2019), <https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment>.

-
- ¹⁸ Merrill Corporation, “GDPR Burdens Hinder M&A Transactions in the EMEA Region, According to Merrill Corporation Survey” (Merrill Corporation, November 13, 2018), <https://www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html>.
- ¹⁹ NiemanLab, “More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect” (August 7, 2018), <https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/>.
- ²⁰ Joseph O’Connor, “Websites not available in the European Union after GDPR” (March 20, 2019), <https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr>.
- ²¹ CNN Business, “These companies are getting killed by GDPR” (May 11, 2018), <https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>.
- ²² Center for Data Innovation, “The EU’s Right to Be Forgotten Is Now Being Used to Protect Murderers” (September 21, 2018), <https://www.datainnovation.org/2018/09/the-eus-right-to-be-forgotten-is-now-being-used-to-protect-murderers/>.
- ²³ Ship Your Enemies GDPR, “Ship Your Enemies GDPR,” (n.d.) <https://shipyourenemiesgdpr.com/>.
- ²⁴ Daniel Castro, “The Pandemic Reveals Some of the Noxious Side Effects of the GDPR,” April 14, 2021, Center for Data Innovation, <https://datainnovation.org/2021/04/the-pandemic-reveals-some-of-the-noxious-side-effects-of-the-gdpr/>.
- ²⁵ Jasper Bovenberg et al., “How to Fix the GDPR’s Frustration of Global Biomedical Research,” *Science*, October 2, 2020, Vol. 370, No. 6512, pp. 40-42, <https://www.science.org/doi/abs/10.1126/science.abd2499>.
- ²⁶ “The BIPA Litigation Landscape and What Lies Ahead,” Woodruff Sawyer, April 1, 2021, <https://woodruffswayer.com/cyber-liability/bipa-litigation-landscape/>.
- ²⁷ “CCPA Litigation Tracker, Updated as of December 2021,” Perkin Coie, n.d., <https://www.perkinscoie.com/en/ccpa-litigation-tracker.html> (access February 14, 2022).

The CHAIRPERSON. Thank you very much, Mr. Castro, and to all our witnesses.

We will go now to Members of the Committee who may have questions, and I will turn first now to our Ranking Member, Mr. Davis.

Mr. DAVIS. Thank you, Madam Chairperson.

And thanks again to our witnesses. Enjoyed your testimony.

Mr. Castro, let me start with you.

There have been proposals introduced in Congress that if implemented would create a private right of action for individuals and a collective right of action for certain nonprofits to sue on behalf of individuals. Is this the best approach to ensure protection and accountability for a Federal data privacy framework?

Mr. CASTRO. No, I don't think it is. Right now, we have a very effective regulator in the FTC and we have State attorney generals that can obviously also take up that slack.

What we have seen in States that have implemented these private rights of action, like with the Biometrics Information Privacy Act, once a court ruled that you could bring lawsuits under this for cases where there is no actual harm to consumers, we saw a flood of lawsuits. And these lawsuits are being driven by class action lawsuits where they are just going after the attorney fees, and this has led to very significant fines without any real payoff for consumers.

So, in the past year we have seen over \$100 million in settlements for companies like Facebook, ADP, Walmart, Six Flags, Wendy's, TikTok, and the list goes on. And these aren't instances, again, where we have seen any consumer harm. It was pure technical violations.

That is not an effective use of dollars that could be going back into investing in technology and processes that would protect consumers' privacy, make it more secure, and protect them from harm.

So, a private right of action, to me, is just taking money out that could be used on actual protections for consumers.

Mr. DAVIS. Well, thank you, Mr. Castro.

Hey, I am sure you have read the media reports about Special Counsel John Durham's allegations that Democrat political attorneys perhaps, Marc Elias specifically, infiltrated servers at The Trump Organization and at the White House.

Would nationwide data privacy legislation have protected President Trump from these data espionage attempts?

Mr. CASTRO. Well, it depends. Certainly, privacy legislation would restrict what companies might be able to keep on hand and what they might share.

But at the end of day, what you really want to see if you want better security is better transparency, so consumers know what they are getting. In this case, The Trump Organization, the Trump campaign, would know what kind of security and privacy controls they are getting when they purchase a service, and they will know how their data could be shared.

And so, getting more transparency is really what we should be looking for in the future.

Mr. DAVIS. Well, I agree, transparency matters. But so do penalties for bad actors if these allegations are borne out.

Do you know if the FTC would have any enforcement penalties if these allegations were borne out?

Mr. CASTRO. The FTC can impose penalties on companies for violations. Particularly the way this works right now is most companies have statements in their privacy policies, their terms of service, that say, we respect your privacy, and we are going to secure your data. And when they do not do that, that is a misrepresentation, and the FTC can and has gone after companies for that.

We can certainly consider giving the FTC more authority. Certainly, if we are increasing their budget, I think we should be saying exactly what we want them to be doing with that additional money. I think that is the best way to go forward.

What we don't want to do, I think, is give the FTC too much latitude, though, to start doing its own rulemaking that goes outside of congressional intent, because it becomes very risky, that the FTC might decide that they want to start deciding how companies should design their websites or how they should be designing their mobile apps, all under the name of maybe ensuring consumers aren't being manipulated. But on the other hand, the FTC is not made up of engineers and user experience designers.

Mr. DAVIS. Very good points. But this agency does exist to address concerns already.

The Online Privacy Act of 2021, a bill referred secondarily to this Committee, calls for the creation of a new Federal agency called the Digital Privacy Agency.

Not only is this a clear example of Congress shifting its legislative authority to the executive branch, but it also seems like an extreme waste of resources given the existing structure already established in the Federal Trade Commission and with the States' attorneys general.

Mr. Castro, do you believe that a new Federal agency is necessary to accomplish the goal of data privacy?

Mr. CASTRO. I think the FTC has the authority it needs and the reputation and experience to do this job. I don't think we need a new agency to solve that problem.

I would also mention that when we think about protecting consumer privacy, this overlaps with fraud and security, and that is something the FTC is also focused on or should be focused on. And I think if we split up that mission, we weaken protection for consumers.

Mr. DAVIS. Well, Mr. Castro, thanks for joining us, and to all the witnesses.

I yield back the balance of my time, Madam Chairperson.

The CHAIRPERSON. Thank you.

Mr. Raskin, you are now recognized five minutes.

Mr. RASKIN. Thank you, Madam Chairperson.

Ms. Fitzgerald, I was eager to ask you the question about the aggregation of data, about how the aggregation and processing of data in large quantities can pose risks that might not be apparent when we are just talking about a single piece of discrete information. I am wondering what can be done about that.

Ms. FITZGERALD. Thank you, Representative Raskin.

I think the lesson we can take from all these data points being combined about us is, one, it shows how important it is to have a

comprehensive privacy law that covers personal data generally rather than the sectoral laws—HIPPA, FCRA, COPPA, FERPA, the acronyms go on and on—that leave huge gaps in protection for personal data not covered by those laws.

And these flows of personal data also show why notice and consent doesn't work. The breadth of the commercial surveillance industry is just impossible for the vast majority of internet users to fully grasp. A user may consent to have the website they are visiting use their data, but does that mean they are consenting to that data being passed on to hundreds of data brokers they have never heard of?

We saw an example of this last summer when a Catholic priest was outed by a news outlet who obtained supposedly anonymized location data from the dating app Grindr. I know that following that revelation you and Rep. Porter sent a letter to the FTC and FCC, signed by a few members of this Committee, asking them to conduct a rulemaking to strengthen privacy protections for location data. And that is something that could also be integrated into privacy legislation.

Mr. RASKIN. Thank you much.

Ms. Zuboff, I have read your book about surveillance capitalism. I know it is hard to synthesize an entire book, but who is Big Brother today? Is Big Brother the state as we have traditionally conceived it, or is Big Brother corporate—the corporate sector, or is it some combination thereof?

Ms. ZUBOFF. Well, thank you so much, Representative Raskin. I am flattered and thrilled to hear that you have read my book. So, thank you for that as well.

As you know, because you have read the book, I develop a concept that I call Big Other. So Big Brother was a notion of a totalitarian state, which had a very specific ideology and wanted people to believe certain things and talk in certain ways and act in certain ways.

We have surveillance capitalism, not a totalitarian state. Surveillance capitalism really doesn't care what you think. It doesn't care what you believe. It doesn't care how you act.

What it does care about is that you think and believe and act in ways that it can capture the data to do the aggregation that you are asking about, because with that aggregation is the possibility of computation, applying artificial intelligence, coming up with predictive algorithms, targeting methodologies.

With those targeting methodologies, various functions are achieved, including increasing engagement, which is a euphemism for increasing the footprint for greater data extraction.

And also, as we increase engagement, using our knowledge from this deep computation, AI, using our knowledge about you for things like subliminal cues, psychological microtargeting, engineered social comparison dynamics, so we really, really know a lot about you.

And that way we can use messaging and different—not only the content of messaging, but the forms of messaging, to actually begin to modify your behavior, and to do that in a way that is consistent with the commercial objectives of the company and its business customers.

So, at the end of the day, this Big Other is a—sorry. I will just wrap it up with the notion that this Big Other is ubiquitous, is pervasive, it is not totalitarian, but it is full-on control, and full-on opacity, full-on power.

Mr. RASKIN. We haven't yet enacted a comprehensive Federal privacy statute to address the rise of the Big Other. But a lot of States and some other countries have attempted to do so.

I wonder if you can just tell us what you think have been the best lessons and the best efforts at a comprehensive privacy framework to protect us individually, but also to protect the people's possession of interest and ownership of their own characteristics and their own behavior.

Ms. ZUBOFF. Well, the gold standard right now, and we couldn't have said this a few weeks ago, but the Digital Services Act and the Digital Markets Act in the EU. These are not the total solution. We have very specific things to accomplish ahead of us.

As far as setting a new standard, defining a new frontier for the kinds of rights—when I use the word “users”, I try to do it with air quotes, because users is all of us. Users is kind of the synonym for humanity at this point.

And these pieces of legislation, they are ambitious, they are comprehensive, they have the buy-in of the European Parliament now and the member states. A few details left to be worked out in the spring.

But these set a new standard for rights of users, the enforcement powers of a government to really for the first time put democratic governance back in control of our information and communication spaces, to work with the private sector, rather than have the private sector as what it has been for the past two decades, a completely autonomous force, essentially unimpeded by relevant law.

And all the social harms that we have been describing this afternoon are the result of that situation.

The CHAIRPERSON. Thank you so much. And the gentleman's time has expired.

We will turn now to the gentleman from Georgia, Mr. Loudermilk for five minutes.

Mr. LOUDERMILK. Well, thank you, Madam Chairperson.

And it is a very interesting topic that we are talking about, I have been dealing with for quite some time.

Mr. Castro, one of the issues that I have seen from a financial services perspective, and I assume it is going to be the same here, is the multitude of data privacy standards and laws we have across the country in the different States.

You mentioned in your testimony that there were 34 State legislatures that introduced bills in the space from 2018 to 2021. I want to get your thoughts on the importance of having a uniform Federal standard for data privacy that would go across the board.

Mr. CASTRO. Yes. I really appreciate that question. Thank you so much, Representative Loudermilk.

For I think so many companies, especially the smaller companies, when you think about data privacy, we are often—I think the first thing people think about are Facebook and Google.

But these laws impact everyone. They impact the local florist, the barber shop, the grocery stores. And complying with those laws

can be very expensive and very difficult, because even though at the end of the day most of these laws are basically saying the same thing, they say it all a little differently.

And actually, complying with those laws so that you are not held in violation, so that, especially if there is a private right of action, so that you are not sued for making technical violation if you have not, for example, put a certain term up on your privacy policy on your website, you might be in violation of California's law.

All these obligations add costs for businesses. And these businesses, instead of hiring another engineer or giving a raise to their workers, they must go out and hire a privacy lawyer. A lot of the privacy lawyers really like privacy laws because it is good business for them.

And the issue here is we don't need more laws, we need one good law. I am glad to see we are having this conversation, because I think we can get to that one good law. Hopefully we can get there sooner rather than later, because the more we wait the higher those costs get.

Mr. LOUDERMILK. So, what kind of effect does this have on American competitiveness in the international marketplace?

Mr. CASTRO. It is very significant right now. When we think about—a lot of U.S. companies are doing a very good job with protecting privacy better than, for example, companies in China. But because the U.S. does not have a Federal law and we have taken a sectoral approach and other countries have not taken that sectoral approach, a lot of countries will say the U.S. doesn't care about privacy.

I don't think that is true. I don't think that is true in terms of when I hear the FTC defending the work that they are doing. I think they are doing very respectable work. I think the State attorney generals are doing great work. I think some of the State laws can even be effective.

And so, I don't think it is fair to say the U.S. isn't doing good work on privacy. But we don't have a national privacy law. And so, so often that fact is used to say a U.S. company should not get a particular contract.

We are seeing that used right now. That is hurting transatlantic data flows in part because European lawmakers are saying the U.S. isn't doing enough to protect consumer privacy.

So, I think one of the best ways we can promote U.S. competitiveness, again not just from the tech sector but across the board, is to create this Federal law so that we can show the U.S. is taking this seriously.

Mr. LOUDERMILK. I think everybody on this Committee is committed to and I think most individuals recognize the importance of protecting personal data and an individual's privacy. Definitely, I do as well, and I know you do.

But with that being said, you mentioned in your testimony a concern that I share as well, which is the compliance cost to small businesses due to State privacy laws.

Is there a State that you can point to that has successfully executed a data privacy law that balances those concerns?

Mr. CASTRO. I think Virginia is probably the closest we have gotten so far. They are trying to strike the right balance.

Again, the biggest problem is that when you see these State laws, the State legislatures are not thinking about the costs that would be borne by States outside their borders.

And so, again and again, as we see each new State go down this path, they are putting up laws that force companies to go rehire lawyers, to ask them to reevaluate their privacy policies, make technical changes to their systems, all the same compliance, again, without any discernible improvement in actual consumer privacy.

And so, if the goal is consumer privacy, let's address this top down rather than have fifty different rules for how to do it and have so much more consumer confusion about what is going on and who is protecting your data.

Mr. LOUDERMILK. All right. I agree wholly.

I see my time is quickly running out. So, thank you for that.

And, Madam Chairperson, I yield back.

The CHAIRPERSON. The gentleman yields back.

Mr. Aguilar is recognized for five minutes.

Mr. AGUILAR. Thank you, Madam Chairperson.

Mr. Erwin, I wanted to talk with you a little bit about the lessons that Mozilla has learned from its own experience in building privacy-protective tools. That may be relevant to us here in the public sector and for government agencies that we have oversight over to consider how they are going to handle personal information and to minimize risk for their own operations.

What are your thoughts on what you have learned and what is applicable to the public space?

Mr. ERWIN. Yes. So, I think there are two important ways that we approach this question.

The first is to think about, like, our core privacy practices and the data that we are going to collect from our consumers and how we are going to be really transparent and provide them with control of that.

We really work hard to sort of follow these what typically is referred to as data-minimization practices where we are really only collecting what we need to run our business and optimize and build a great product for our users.

And that is a practice that, frankly, isn't followed very expansively across our industry with the underlying problems that I think that we see and really think needs to be fixed.

And then once we have that data, we will work to protect it aggressively, which is I think basic applicability of this idea of data minimization, and plus sort of a strong set of security controls on the back end is one that really needs to apply both to the public and the private sector.

We also work hard to build kind of what I mentioned earlier, these privacy features into the browser that protect our users from web encryption, blocking, tracking in the browser.

The interesting thing that—experience we have there is, like, that can be a little bit disruptive for the industry in a way that, like, right now we have a permissive internet, many parties that depend on that permissiveness to build their data practices and build their business.

That is fundamentally actually a problem. And so, some amount of disruption is healthy. We don't always get a positive response

when we roll out privacy features. I think that is a positive signal that we are going in the right direction. But it certainly creates a little bit of headwind for us when we try to roll out privacy features.

Mr. AGUILAR. Understood. Sometimes being at the forefront means that you take on a lot of folks with differing viewpoints as well.

Ms. Fitzgerald, what are some of the best ways that we can limit the risks and harms of the aggregations of personal information over time from multiple different sources that we know exist?

Ms. FITZGERALD. Thank you, Representative Aguilar.

I think this process of data minimization that has been talked about a few times, especially in the first panel, I was thinking if private companies treated our data like the GPO did, we would be in much better shape. The point was made, if you don't have it, you don't have to protect it.

So, the obligation should be on the companies to minimize the amount of data they are collecting, delete it when they don't need it anymore. That protects users from having their information passed on and it protects them in the case of a data breach.

Mr. AGUILAR. Thanks. I appreciate that.

Mr. Erwin, back again, what are some of the privacy risks and harms that we have that may not have a primarily technological solution? I guess what I am trying to ask is issues that instead require changes to business practices or laws. We are trying to balance the regulatory side here, and I wanted your thoughts on how we balance those pieces.

Mr. ERWIN. Yes. So, we bump up against this problem all the time in our work in the browser where, for example, the challenges that we can solve, a user visits a website, for example, and there is a hidden third party on that website that the user doesn't know about and is collecting data about them.

That is a third-party relationship. We can do something about that in the browser, because typically there is, like, a network request, to get a little bit technical, that calls out to that third party. So we can actually just block that.

So that is typically the role of, like, the browser, or the operating system can jump in and say, we are going to prevent these third parties from sort of tracking your behavior.

What we can't do as much of is when the user has a direct, first-party, what we refer to as a first-party relationship with a website or business. And that comes down to a question of business practices, not technical problems. And there is little we can do to sort of adjudicate the relationship between a user who has decided to engage directly with a first-party business, but that business isn't upstanding, and the user might not know about it.

And that is where I think law and regulation really needs to step in where the technical fixes ultimately aren't going to get us what we need.

Mr. AGUILAR. I appreciate that. Thanks so much. I yield back.

The CHAIRPERSON. The gentleman yields back.

Mr. Steil is recognized for five minutes.

Mr. STEIL. Thank you very much, Madam Chairperson.

I want to pick up where my colleague Mr. Aguilar left off a little bit. But I want to shift over to you if I can, Ms. Fitzgerald, on the topic.

I was reading some of your testimony, and you referenced that the biometric and genetic data is especially sensitive, it deserves stricter regulation. Is that correct?

Ms. FITZGERALD. Yes, absolutely.

Mr. STEIL. And you raised some concerns about how healthcare data is used. Is that correct?

Ms. FITZGERALD. Yes. Health data is particularly sensitive.

Mr. STEIL. And so, I think a lot of people think that HIPPA is protecting their healthcare data, as it extends to big tech or health apps, but that is not correct. Would you agree?

Ms. FITZGERALD. Right. HIPPA only applies to the relationship with your doctor and with your health insurance company and with certain health exchanges, it doesn't cover health data that is in apps.

Mr. STEIL. Yes, I think that is a really interesting distinction that I think a lot of Americans might find interesting, and building on what was previously being discussed with Mr. Erwin on these kind of third-party apps, third-party relationships that exist on certain websites and the impact that this could have.

And so Congress recently passed the 21st Century Cures Act to protect patient data, in particular to require patient data to move from the doctor's office to healthcare apps of the patient's choosing. There are a lot of reasons that is a good thing. There are some things that we want to make sure we get right.

Because you want to be able to make sure patients can control their data. But I also want to ensure that they don't lose control of their data by sending it in a third party that they might not be aware of would find interest in their healthcare data, their biometric data, or others.

Do you think the risk is bigger in some of these apps that might send—that individuals, that the risk might be greater if they are sending information to some of these types of apps kind of under the rules and regulations of the 21st Century Cures Act?

Ms. FITZGERALD. The reason biometric data is so sensitive is because we can't change it. We can't change our face print, we can't change our fingerprints.

Mr. STEIL. So, let's shift off for a second. I totally agree. I think that is a great topic.

Let's shift and talk about medical data. Does that give you unique concern?

Ms. FITZGERALD. Yes, sure, because of the ways it can be used against us. You think about the insurance companies using it to determine our rates or even an employer possibly not wanting to hire someone with a health condition if they are going to be paying their health insurance premiums.

Mr. STEIL. I appreciate your commentary. I think it is an area that we need to just really keep an eye on. I think there is a lot of real positive things. We want to make sure innovation is here in the United States. We want patients to control their data.

But at the same time, we want to make sure that patients are protected, and where there might be a third-party player involved

where the patient might not fully appreciate the risk that they are engaging in, in sharing their data. I just think it is something that we really should spend time and think about.

Let me shift gears if I can. Thank you very much, Ms. Fitzgerald.

Let me shift gears to you, Mr. Castro.

There is a lot of laws that govern privacy for different types of institutions. The Gramm-Leach-Bliley Act Federal law required financial companies to explain their information-sharing practices to their customers and to safeguard some of their data.

And before creating new laws, I think there is a real opportunity for Congress to look at how current privacy laws are working and how they interact with each other so that we are not duplicative of regulations.

And so, could you shine some light, since the passage of GDPR in the EU, what have we seen in that sweeping legislation? Has it stifled innovation? Has it grown innovation? What big takeaway should we take from that, from the EU's work?

Mr. CASTRO. In many areas it certainly has stifled innovation. When you look at the cost of compliance, when you look at the impact it has had on startups in the European tech economy, there are many areas where just the data points again and again show that European businesses are suffering.

The one area——

Mr. STEIL. So let me, Mr. Castro, only because we have got limited time, if we shift gears slightly and we say let's jump over to California.

California Consumer Privacy Act, what lessons can we take away from the State of California if we were to take that and run that out nationally.

Mr. CASTRO. One of the biggest problems with California is we have seen hundreds of lawsuits related to enforcement. That has been a problem.

One of the biggest positives of it is the idea of a thirty-day cure, which I think could be extended nationally, where the goal is not to penalize companies for mistakes, but to get them to take corrective action. That has been——

Mr. STEIL. Thank you very much. Only cognizant of time. I appreciate everybody's time here.

I think what is really important is we have got a lot of laws already on the books, State laws, we can look at the EU, we can look at what financial services committees are doing, we can look at the 21st Century Cures Act. I think it is critical that we are looking at all of these legislations, learning lessons from them, so we can help consumers protect their data, but also maintain innovation here in the United States of America.

I appreciate you holding today's hearing, Madam Chairperson and I will yield back.

The CHAIRPERSON. The gentleman yields back.

Ms. Scanlon is recognized for five minutes.

Ms. SCANLON. Thank you, Madam Chairperson.

I guess I would like to pull on this thread a little bit more since we certainly do hear quite a bit about this on the company side and the agency side: How do they navigate all these different laws that are being promulgated between States, but also between countries,

because, as we are aware, the internet does not have national boundaries in the same way?

So, Ms. Fitzgerald, could you talk about that? What are the most important privacy rights that you have seen that have been proposed that you think Congress should work on adopting?

Ms. FITZGERALD. Well, the most important thing, I think, when you are thinking about privacy legislation is we can't just be telling people what companies are collecting about them. That is not enough. We need to put obligations on the companies that are collecting data to limit that collection, limit what they are doing with it after they collect it and have them delete it when they are done using it.

Ms. SCANLON. Okay. In terms—do you have any suggestions about which are the best models for us to look at, whether there is State models, or the EU has been mentioned?

Ms. FITZGERALD. Sure. So, I think State models, you know, California has the strongest right now in the United States. The CCPA in California is the strongest model we have seen. But, that still is even limited, only allows users to opt out of the sale of their personal data. It doesn't as much put obligations on companies to minimize the data they are collecting.

The Online Privacy Act by Chairperson Lofgren is a great model. That includes data minimization. It also includes provisions protecting against discriminatory uses of data. That is really important.

You also want to make sure you are requiring algorithmic fairness and accountability. We don't want to make the same mistakes with AI that we have made with data collection. This is the next wave of technology. Let's get ahead of it, set the rules now, encourage companies to innovate around privacy and autonomy.

Ms. SCANLON. Okay. I mean, one of the typical—I don't know—tools that people talk about with the privacy laws is the notion of consent. I gather that you are a little bit skeptical about the usefulness of consent as a focus of privacy protections.

Can you talk about that a little bit?

Ms. FITZGERALD. Yes. Absolutely. There is just no way for an individual to understand kind of the web that their data gets passed through if they are consenting. You know, if you are just hitting that consent button to make the banner go away on a website—

Ms. SCANLON. Yes.

Ms. FITZGERALD [continuing]. You don't realize that what you are saying is: Sure, take my personal data and do whatever you please with it. There are no rules.

Ms. SCANLON. Right. Well, and certainly we have seen that proliferate recently with—to get access to almost anything, you either decide to click, or you decide not to—

Ms. FITZGERALD. Exactly.

Ms. Scanlon [continuing]. Protect it.

So, with respect to discriminatory data uses, how do we address that? What are your top-line recommendations there?

Ms. FITZGERALD. Well, groups such as Color of Change, Lawyers' Committee for Civil Rights, Leadership Conference have great proposals on what we need to do to make sure that civil rights are protected online, you know, making sure that—I don't know—public

accommodations are protected; you know, that extends to online spaces.

You need to make sure that the algorithms that companies are using are not being used in ways that deprive people of life opportunities like, you know, ads for housing and ads for jobs, that those are data—our personal data isn't being used to show those in discriminatory ways.

Ms. SCANLON. That is interesting.

Okay. Thank you, Madam Chairperson. I yield back.

The CHAIRPERSON. The gentlelady yields back.

The gentlelady from New Mexico is now recognized for five minutes.

Ms. LEGER FERNÁNDEZ. Thank you so much, Madam Chairperson.

As we have heard today, our personal data is extremely valuable. You know, we take a question, a quiz on Facebook, look up directions. The companies collect our information. They then sell our information, often without our consent, to a third party. And then they use our information—our information—for a range of activities, from showing an ad for clothing, to sometimes more dangerous, like targeting disinformation to manipulate our behaviors or beliefs.

And it is all invisible to the true owners of the data. Me, my neighbors, our fellow Americans, I want to focus a bit on how data privacy or the lack thereof impacts our elections and our democracy. The Elections Subcommittee of this Committee recently held a roundtable in Miami on the creation and dissemination of disinformation about our elections and the pandemic, and this disinformation targets Spanish-speaking communities.

We learned how the disinformation is then exported to other States, including New Mexico, and then amplified based on this data harvesting that we have heard about today and read in this testimony.

Ms. Fitzgerald, you noted that actors can weaponize our data to undermine our election integrity and democratic institutions. In practice, what does this weaponization look like?

Ms. FITZGERALD. Sure. Thank you, Representative Leger Fernández.

You know, just as advertising companies use profiles about us to manipulate us into purchases, you know, so too can they manipulate our views by filtering the content we see. So, the ways they can do that are—you know, The Markup did a great investigation right after January 6th showing the two different Facebooks that Republicans and Democrats were seeing. And it is just a stark view of kind of the different information that both sides are seeing and how that shapes your views.

Even if someone doesn't click through to an article, just seeing that headline, having it in the back of their head as they are voting, it is—these companies are able to kind of manipulate our political views by determining what we see.

Ms. LEGER FERNÁNDEZ. Professor Zuboff, I really appreciated your poignant written remarks about how democracy is simultaneously the only legitimate authority capable of helping the surveillance capitalism but also a prime target. So, I appreciate that

and would welcome you expanding on that, but the question I want to get to first is Mr. Castro suggested that a private right of action is unnecessary and that we should focus solely on transparency.

Do you agree, and, if not, why?

The CHAIRPERSON. You need to unmute, Professor Zuboff.

Ms. ZUBOFF. Sorry.

I don't agree with that. I think the private right of action is very important. When we pass a law, whether it is the California law or any other law, that is only the beginning. What must happen is these laws are tested, and they evolve, and they develop. As a society, we learn what they can mean, what they can mean for us, and how they are going to protect us in society.

So, what the private right of action does is it creates the opportunity not only for individuals, but for groups of people, for collectives to really bring issues into the judicial system, to have those issues explored, and to create precedence.

And this is—you know, this is what is called the life of a law, how the law evolves and how we can move forward into this century, not just with statutes that are frozen in time, but with laws that are evolving according to what Justice Brandeis once called the eternal youth—

Ms. LEGER FERNÁNDEZ. Right.

Ms. ZUBOFF [continuing]. Of the law, because we have these kinds of international processes. So this really is—

Ms. LEGER FERNÁNDEZ. Yes, and I wanted to completely agree. Our civil rights laws would have had no effect if we hadn't had the right of private action.

I did want to ask you, though, to elaborate in the few seconds left with regards to what you believe is most important to protect our democracy in an Online Privacy Act?

Ms. ZUBOFF. Well, the first thing is you notice so much of our discussion has been we minimize data or how is the data used and things like that. Once we start a discussion talking about data, we have already lost primary ground.

The key thing is now that we are all targets for massive scale secret data collection, much of which should not be collected in the first place. The decision should lie—the decision rights should lie with the individual: Do I want to share this information about the cancer that runs in my family, and do I want to share that with a research operation or a federation of researchers that are going to make progress on this disease and help the world? Maybe so.

But do I want Google or Facebook or any other company to just be inferring information about my cancer from my searching and my browsing? Absolutely not.

So we need to reestablish decision rights, as Justice Douglas offered in 1967, the idea that every individual should have the freedom to select what about their experience is shared and what remains private. These decision rights are the cause of which privacy is the effect.

We need to establish now finally in law juridical rights that give us the choice of what is shared and what remains private. Then we have got a whole new ball game where all kinds of innovations like Mozilla and all of the Mozillas that are waiting to come on stream,

not just obviously in search and browse, but in all kinds of businesses, in every sector.

Ms. LEGER FERNÁNDEZ. Thank you.

Ms. ZUBOFF. We are all waiting to get in the game.

Ms. LEGER FERNÁNDEZ. Thank you. I know we have overgone our time limit.

Thank you, Madam Chairperson——

Ms. ZUBOFF. Thank you.

Ms. LEGER FERNÁNDEZ [continuing]. And I yield back.

The CHAIRPERSON. The gentlelady yields back.

I just have a few final questions.

First, thanks to all of the witnesses for really very excellent, interesting, and enlightening testimony.

I wonder, Mr. Erwin, in your testimony, you refer to dark patterns as one of several privacy abuses that demand regulation, that technology alone couldn't adequately address them.

Can you explain in further detail for the Committee and for those watching this hearing what dark patterns are, what are some of the most troubling examples of dark patterns, and what is the best legal approach to reining them in?

Mr. ERWIN. Yes. A dark pattern is a sort of broad umbrella term used to refer to what is typically sort of user experiences that can deceive a user into opting into data collection or consenting to data collection without being explicit about what is really happening under the hood. And that can be—a dark pattern could be sort of text that is intended to deceive the user, or it might be sort of if you have got to click through five things to opt out of the data collection. All of those, I think, are typically—are sometimes referred to as dark patterns.

We see those everywhere across the web. And, as I mentioned, that is the type of area where the browser can't really do much when the user is actively engaging with the first party. It is an area where I think we really do need to see some regulatory engagement.

Obviously, like, we don't want a regulator designing a user experience in the browser. Sort of our user experience team doesn't want me designing the experience in the browser, so we definitely don't want a regulator doing that. But actually, acting to say here is what the standard should be, and here is what looks like a deceptive practice, and here is what is a sound practice; that is where I think we really do need to see a regulatory voice.

The CHAIRPERSON. Standards instead of design?

Mr. ERWIN. Yes.

The CHAIRPERSON. You know, we have talked a lot about the rights of individuals for privacy and, you know, some of the disinformation, digital addiction, harmful impacts on children on certain internet platforms. But I think whether there should be a private right of action.

I think the core issue really, as Mr. Halpern said, if you don't have the data, you can't use it to manipulate. And I think—it is my view that the victims of manipulation, whether it is for political, societal, cultural, or commercial purposes, it is not just the individuals being manipulated but the public at large.

If you are manipulating for a commercial purpose, you are a Big Tech company and you have got all this data, you know, you are at an unfair advantage to smaller companies that have not acquired all that data. If you are manipulating for a cultural or societal purpose to move society in one direction or another, the public is also a victim of that. Individuals have been removed from their agency and have been — and are less free because a private corporation is manipulating them through their own data.

So, let me ask you, Ms. Fitzgerald, isn't really the crux of this to restrain the collection and retention of data?

Ms. FITZGERALD. Yes, absolutely. It is not enough to—for users to just know what companies are collecting about us. It has to be restrained. The obligations have to be on the data collectors to limit what they are collecting.

The CHAIRPERSON. I just want to mention briefly—and maybe any of the witnesses can talk. Ms. Fitzgerald, you may have studied this in your nonprofit. You know, I am a fan of the FTC, but I have been advised by many who served there that the sheer number of individuals who are really technologically savvy is fairly minimal compared to the actual army of digital, you know, engineers, software-savvy people in these large companies, and that, frankly, they are no match for the gigantic companies with the computer and digital expertise that those companies have, which is why we are looking at how do we better arm a regulatory agency to actually be successful in facing off with these gigantic corporations?

Is that capacity of the FTC off base, Ms. Fitzgerald, in your view?

Ms. FITZGERALD. Absolutely. I mean, look, we are encouraged by recent actions at the FTC on privacy, but the FTC has limited resources and an incredibly broad mandate that covers everything from antitrust to horse racing safety, tractor parts, and laundry tags. The task of data protection is best done by a specialized, independent regulator. When you think about the outsized presence of technology in our lives and our economy, I just think this is something where, twenty years down the line, no one will question why we have a data protection agency just as now we don't question why we have an FAA or an EPA.

The CHAIRPERSON. Let me just ask a question of you, Mr. Erwin. In your written testimony, you state, quote, "it is important that competition concerns not be a pretext to prevent better privacy for everyone."

Can you explain that tension and how Congress might strive to strike the right balance on that?

Mr. ERWIN. Yes. I mean, this is something we see often. Again, like the basic challenge we have here right now is the internet was designed in a very permissive way, and that allows for a large diversity of parties to collect data.

In some cases, those are the largest parties, but also the smaller ones. And closing down some of these privacy gaps necessarily means denying data to both the big parties and the small ones. And sometimes we will hear this argument that we shouldn't close the privacy gap because that will have certain competition implications.

We really sort of reject that stream of thinking, the basic idea being that, like, we should leave the internet being more permissive in order to protect some set of business models.

You know, what we want to see is an overall but more protective platform that has an even playing field that all big and small companies can compete on. That is the approach that we, I think, are in favor of. We are going to push back aggressively on any suggestion that we should leave privacy holes in the browser or in your operating systems in order to protect some certain business model that might be competing against Big Tech.

The CHAIRPERSON. Right. I will just close with this.

I live in California. The California law has not really stopped the kind of collection that I think its authors intended.

I will say, however, that, despite some decrying the regulation, the formation of businesses in the tech sector is at an all-time high. Business is good. Actually, job creation in Silicon Valley is carrying the entire State. So, it has not had these horrible impacts in the tech sector.

I am mindful that, if we constrain the collection and retention of data by internet companies, especially in the internet space, it will require a change in their business models. I think that is necessary because, right now, the propensity and the capacity to manipulate every person in America is unacceptably high.

So, I am wondering, Professor Zuboff, you talked about, in your New York Times essay recently, about how democracies are confronting the tragedy of the uncommons and how we need to get back to protect our society, for lack of a refined thing.

Can you expand what is the most important thing to accomplish that goal in your judgment?

Ms. ZUBOFF. Well, you know, the digital century opened with great promise. It was supposed to be the democratization of knowledge. I am not ready to let that dream die.

The problem is we have gone on this kind of accidental path. In my written testimony, I gave a lot of background as to how that happened. A certain market ideology, certain national security concerns, the accidents of financial emergency in Silicon Valley, and how surveillance capitalism was invented in order to get tiny little Google in the year 2000, you know, over the hurdle when its investors threatened to pull out in the dot-com bust—a bunch of accidents, and that is why I call where we are an accidental utopia.

But what we really have is an opportunity for the digital century to be a century where data is being used to further the needs of society, to solve our core, most important problems. And data collection is being used in ways that are aligned with what we consider in the digital century to be necessary fundamental rights.

This is work that we have not yet undertaken. We have got to figure it out. It would be like having lived through the 20th century without ever having tackled workers' rights or consumers' rights and the laws to oversee those rights and the institutions to oversee all of that. We created all that in the 20th century.

We are in a new century, new material conditions, new kind of capitalism. We have got to do that fundamental creative work all over again. And that, finally brings us to a point where right now, there is this very in-depth census of how artificial intelligence is

developing around the world, the ecosystem of artificial intelligence, and what it shows very plainly is that the five Big Tech companies own almost all of the artificial intelligence scientists, the science, the data, the machinery, the computers, everything pertaining to artificial intelligence is concentrated in a small handful of companies.

All of that knowledge and capability and material is going to work to solve the commercial problems of these companies and their business customers—surveillance capitalism. It is not being used for society.

So, the public is being—not only is agency being subtracted from individual life, but the benefits of the digital are being sequestered from the life of our publics, our societies, our democracies. We have the opportunity to get that back and get us back on track to a digital century that actually fulfills its promise of knowledge, democratization, and really solving the problems that face us. That is what it is all about.

The CHAIRPERSON. Thank you so much, Professor.

And thanks to all of our witnesses.

As I mentioned, the record of this Committee will be held open for at least five days. The Committee may have additional questions for you, and, if so, we will send them to you and humbly request that you answer them. I think that we have advanced our knowledge of this situation substantially today, and it is due to the very helpful and thoughtful testimony provided by these excellent witnesses.

At this point, our hearing will be adjourned, and we will see the Members of the Committee tomorrow for our oversight hearing of the Capitol Police.

So, with that, without objection, this hearing is adjourned with thanks.

[Whereupon, at 4:22 p.m., the Committee was adjourned.]

QUESTIONS FOR THE RECORD

COMMITTEE ON HOUSE ADMINISTRATION
FEBRUARY 16, 2022, HEARING: "BIG DATA: PRIVACY RISKS AND NEEDED REFORMS
IN THE PUBLIC AND PRIVATE SECTORS"
MAJORITY QUESTIONS FOR THE RECORD

Hugh Halpern:

1. How, if at all, has the Government Publishing Office considered potential interactions between the materials it publishes and artificial intelligence technologies -- for example, third parties using AI to mine or process government documents for some purpose? Have possible applications of AI informed GPO's privacy policies or practices in any way?

Yes, because GPO houses govinfo.gov, which receives more than 70 million document retrieval requests each month; maintains the online Catalog of Government Publications; and administers the Federal Depository Library Program (FDLP), we have a good deal of experience with data mining technologies and approaches. AI can make data mining more efficient and increase the likelihood that someone can find the information they're looking for. Conversely, it also increases the likelihood that any Personally Identifiable Information (PII) available online can be found.

Fundamentally, what GPO seeks to do is to redact and suppress Personally Identifiable Information (PII) that may appear in our collections and those other collections that can be accessed through GPO's overall system of online access. With respect to "born digital" content, we aim to do this contemporaneously with the posting of publications that may contain some incidental PII, but when we look at historical content that may already be online we recognize that we have to be vigilant in finding instances in which PII may be in existing collections. GPO employs contractors to help with this work and our own LSCM staff are adept at finding and remediating such PII. We also collaborate closely with our FDLP partners to make sure they are aware when we locate PII in their collections.

In September of 2019, GPO's Superintendent of Documents issued a policy statement on the redaction of Personally Identifiable Information. That extensive policy can be found [here](#) and it aims to proactively redact personally identifiable information (PII) from content discovered in, or being readied for ingest into, the Government Publishing Office's (GPO) system of online access.

Additionally, some of these same AI and machine learning tools could assist with work to identify and redact PII currently performed by contractors. GPO constantly assesses new technology to protect policy.

2. What are the main ways that GPO coordinates its privacy policies and practices with those of other federal agencies? In your view, is there sufficient coordination on digital privacy issues between agencies -- including those in both the executive and legislative branches?

Government Publishing Office (GPO) takes privacy of its employees, contractors, and customers seriously and in that regard, GPO has established its Privacy Program (GPO Directive 825.41B) that promulgates policies, processes, best practices, and training required to guide GPO employees and contractors to protect the Personally Identifiable Information (PII) and Protected Health Information (PHI) (collectively referred to as PII) during all stages of the information lifecycle — when collecting, storing, using, disseminating, or disposing of PII. The goal is to protect the PII because the loss, compromise, or unauthorized disclosure of PII may potentially lead to identity theft or other fraudulent uses that could result in substantial harm, embarrassment, or inconvenience to the affected individuals and tarnish the Agency's reputation.

GPO researched and reviewed the Federal privacy laws, regulations, and standards and studied how such guidance is being practiced at Federal agencies. This process provided the basis for GPO's Privacy Program that is also driven by the same Federal PII guidelines, memorandums, and publications referencing the Privacy Act of 1974 (as amended), the Office of Management and Budget (OMB) memorandums, and the National Institute of Standards and Technology (NIST) standards. GPO Privacy Program specifically promulgates provisions and best practices published under the following laws, regulations, and memorandums:

- *The Privacy Act of 1974*, as amended, section 552a of title 5, United States Code (Privacy Act). The guidelines and practices published under this Act are helping GPO to promote the following four basic policy objectives:
 - Restrict disclosure of personally identifiable records maintained by GPO.
 - Grant employees & contractors increased rights of access to PII maintained on themselves.
 - Grant employees & contractors the right to seek amendment of the PII maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

- Establish a code of “practices” that requires GPO to comply with statutory norms for the collection, maintenance, and dissemination of records.
- *E-Government Act of 2002*. The GPO Privacy Program utilizes the guidance provided in the E-Government Act of 2002. This law was enacted to improve the use of information technology (IT) and also introduced privacy protections for Federal IT systems. Section 208 of the E-Gov Act has two privacy centric provisions, sections 208(b) and 208(c). The first provision requires the completion of a privacy impact assessment (PIA) for all new IT systems, or when major changes are made to existing systems. PIAs identify and mitigate privacy risks of the information system, more fully described below. The second provision requires agencies to maintain privacy policies on their websites and in machine readable format. GPO practices E-Government Act of 2002 by developing PIAs for all systems handling PII.
- Office of Management and Budget (OMB) Memorandum M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, July 1, 2016
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- National Institute of Standards and Technology (NIST) Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010

With regard to the second part of this question, GPO coordinates extensively with our Executive, Legislative, and Judicial Branch counterparts on a wide range of IT, cybersecurity, and privacy issues, and always welcomes opportunities for enhanced collaboration. From our perspective, the level of engagement on these issues is and has been robust in recent years, and we don’t have anything additional to

recommend at this time. At the same time, we will be happy to pursue any recommendations for expanded engagement if proposed by Congress or the Administration.



Majority Questions for the Record

Caitriona Fitzgerald

Deputy Director, Electronic Privacy Information Center (EPIC)

Hearing on "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors"

Before the

House Committee on House Administration
United States House of Representatives

September 29, 2022

Thank you for the opportunity to respond to your questions for the record concerning the privacy risks from Big Data and the need for reform in both the public and private sectors. My name is Caitriona Fitzgerald, Deputy Director at the Electronic Privacy Information Center, or EPIC. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For over 25 years, EPIC has been a leading advocate for privacy in both the public and private sectors.

1. Major digital privacy bills have been introduced in successive Congresses for more than a decade, but they have seen little-to-no progress despite nearly every stakeholder and advocate calling for at least some form of legislative action. In your view, what are the main substantive stumbling blocks to the enactment of a comprehensive federal framework, and how might those be resolved?

At the time of this Committee’s hearing in February, the most recent legislative negotiations had broken down over two stumbling blocks: preemption and private right of action. But in June, leaders of the House Energy & Commerce Committee and Senate Commerce Committee introduced the American Data Privacy and Protection Act (“ADPPA”),¹ a bipartisan bill that would establish important protections for all individuals in the U.S. and strikes a compromise on these issues: it includes a private right of action with certain restrictions, as well as a ceiling preemption provision with certain carveouts.

As with most political compromises, these measures have been criticized by many stakeholders. But the political reality is that more than ten years of concerted effort to reach a deal for comprehensive privacy legislation had failed until this compromise was struck in the ADPPA.

EPIC has long argued that federal privacy laws should set a floor, allowing states to enact stronger protections. We still believe this is the best approach and would prefer that the ADPPA took that approach, but we recognize that compromise is necessary to enact a national standard that would protect the privacy and civil rights of all Americans.²

¹ H.R. 8152, 117th Cong. (2022).

² See Alan Butler and Caitriona Fitzgerald, *Evaluating the American Data Privacy and Protection Act*, Tech Policy Press (Aug. 8, 2022), <https://techpolicy.press/evaluating-the-american-data-privacy-and-protection-act/>.

- 2. While Congress has deliberated on digital privacy, many other jurisdictions have enacted their own privacy laws, both in U.S. states and other countries around the world. What are the main lessons that we should take from these other efforts? What successes should be duplicated in U.S. federal legislation? What should be done differently?**

Despite having a strong rights-based approach and broad geographic impact, Europe's General Data Protection Regulation has faced criticism for its indeterminacy and a lack of strong enforcement.³ That is why it the primary lesson Congress should take from the EU's experience with the GDPR is that a U.S. privacy law must establish clear and comprehensive rules backed by robust enforcement. Congress should establish an independent Data Protection Agency ("DPA") in the United States to regulate, enforce, and coordinate data protection policies across all industries and governmental entities. The DPA must be adequately funded and have strong rulemaking authority. The DPA should have the authority to:

- Investigate violations of the law, audit business practices, obtain preliminary and permanent injunctions, issue cease-and-desist orders, impose civil penalties, and secure equitable monetary relief.
- Require changes to harmful business practices, including banning serious or repeat offenders from engaging in certain lines of business.
- Conduct ongoing oversight over companies who have violated data privacy laws, including by conducting random audits.
- Regulate high-risk data practices, ensuring data processing and algorithms are fair, just, transparent, and non-discriminatory;
- Conduct investigations and adjudicate or otherwise act on complaints from consumers;
- Impose data protection standards and promulgate guidelines and policies for use by the private sector;
- Order disgorgement of data & algorithms; and
- Impose personal liability for executives for deliberate violations.

The California Consumer Privacy Agency is a good model for what a U.S. DPA could look like. State attorney general and private enforcement via a private right of action with stipulated damages should serve as complementary enforcement tools.

³ See, e.g., Ilse Heine, Ctr. for Nat'l Sec. Studies, *3 Years Later: An Analysis of GDPR Enforcement* (2021), <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement>.

State laws in the U.S. have also provided some lessons learned. Laws in California, Colorado, Connecticut, Utah, and Virginia have generally applied either “opt-in” or “opt-out” frameworks — a requirement that companies must either ask for affirmative permission for secondary processing, or that they must give consumers the ability to turn off secondary processing. Both models can be flawed in practice: opt-in models can overwhelm consumers with constant requests for permission and are often manipulative.⁴ Meanwhile opt-out regimes are both difficult to use and wildly impractical if one is to protect oneself in any meaningful way, if consumers have to manually opt out of secondary use for every website, app, or business they interact with, which can amount to thousands of organizations.⁵ As a result of both approaches, consumers are forced to take too many steps to safeguard their data. A better model would be to require businesses to minimize the collection, use, and transfer of personal data to that which is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the individual to whom the information pertains.

- 3. In recent years, both the legislative and executive branches have devoted increasing attention to fostering competition in online apps, services, and platforms. How does this goal interact with the protection of digital privacy? Can privacy and competition efforts conflict with one another -- for example, in requiring that a platform provide third parties with access to user data -- and if so, how might Congress balance these goals?**

A handful of technology companies now assert unprecedented control over the digital economy. Google and Facebook achieved their dominance through unrivaled access to consumer data. While these two companies may be known for offering search and social media services to Internet users, their real customers are advertisers, and the products they offer are the users. Over 80 percent of Google’s revenue comes from advertising,⁶ while advertising accounts for nearly all of Facebook’s revenue.

⁴ *Most cookie banners are annoying and deceptive. This is not consent.*, Privacy International (May 21, 2019), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.

⁵ *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Rights*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

⁶ Pares Dave and Nivedita Balu, *Google search ads beat targets despite global 'uncertainty'*, Reuters (July 26, 2022), <https://www.reuters.com/technology/google-parent-alphabet-posts-higher-quarterly-revenue-2022-07-26/>.

The more dominant these companies become, in turn, the greater their ability to collect consumer data and increase their share of the market. The consolidation of user private data into the hands of a small group of firms is not good for individual privacy or for privacy innovation. Therefore we need new rules that counter this anticompetitive trend while ensuring that the disclosure of personal data for purposes of interoperability is limited by setting strong data minimization rules. Privacy must be a central consideration when developing interoperability rules.⁷

⁷ Bennet Cyphers and Cory Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability* (Feb. 12, 2021), <https://www.eff.org/wp/interoperability-and-privacy>.



27 May 2022

**Marshall Erwin, Chief Security Officer
Mozilla Corporation**

**Committee on House Administration
United States House of Representatives**

**“Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors”
Questions for the Record.**

1. How has Mozilla's experience designing privacy-enhancing products for consumers informed its views of user consent and user decision-making in privacy law? In crafting a comprehensive federal framework, how should Congress balance user choice and flexibility to share data with third parties against the practical risks that consent will be manipulated, uninformed, etc.?

Consent should remain a *part* of the solution to protect people's privacy. However, unlike existing privacy laws which merely require some form of consent, we believe that the bar for consent must be raised, such that consumers have clear and simple choices, presented in a manner that enables them to make meaningful decisions about personal data. We know, for example, that consumers are not given meaningful opportunities to understand how their data is used or what their choices are when they are overloaded with technical information buried in lengthy privacy policies. And yet this is the industry norm today in which consumers are required to "agree to" companies using their data in multiple ways prior to using any new service and again on new product updates. Privacy policies serve important functions as disclosure documents. More importantly, however, we believe it is better to engage people so they are informed at the time that it is relevant, of data collection and sharing that would be privacy invasive or risky.

At the same time, consumers cannot reasonably be expected to make informed decisions based on complicated technical information about data collection, usage and sharing; especially when these decisions must be made continuously and daily with every consumer interaction with a company or product. This places the burden of privacy on consumers. It is much better, we believe, for federal law to *protect* consumers by requiring companies to offer privacy, security, and transparency by default. This should be complemented by strong consumer

rights and clear rules for companies to limit and disclose how data is collected and used.

Our experience within Firefox has shown us that leaning too heavily only on consent will often leave consumers at risk. We know that privacy risks are often opaque and silent and the technology underpinning those risks is often too complex for even subject matter experts to understand. These challenges are compounded by the fact that consent flows are riddled with dark patterns that trick people into data collection and/or push them to use affiliated services over competitors. Recent research shows both the [form](#) these design practices can take, and also the direct [harm](#) suffered by consumers. In the case of a web browser, consumers cannot be expected to make separate choices about third-party trackers on each website that they visit. They have neither the time nor the knowledge to do so.

2. Some have called for a right of personal data ownership in privacy legislation, drawing on concepts from intellectual property law. What view, if any, does Mozilla have of such proposals?

Privacy legislation must include strong baseline rights for consumers that place people in control of their data and privacy. This should include the right to access, rectify and delete data, along with data portability rights that allow consumers to export their data and potentially move it to another platform.

However, we are more skeptical of some privacy proposals that would hew too closely to intellectual property law and that would create a right of personal data ownership. While interesting in concept, such proposals run the risk of making problems within the data economy worse, encouraging people to own and then license their data to third parties that might not have the operational skill or interests sufficient to really protect people's privacy. We believe these ideas, along with concepts like data trusts and data fiduciaries that would serve as holding entities for the data people own, require more examination and exploration before they are incorporated into privacy legislation.

COMMITTEE ON HOUSE ADMINISTRATION
FEBRUARY 16, 2022, HEARING: "BIG DATA: PRIVACY RISKS AND NEEDED REFORMS
IN THE PUBLIC AND PRIVATE SECTORS"
MAJORITY QUESTIONS FOR THE RECORD

Daniel Castro:

1. Your testimony calls for federal privacy legislation that would establish "basic consumer data rights." Would you support minimization in the collection, retention, sharing, and/or use of personal data as one of these rights? If so, how should Congress craft a minimization right?

Establishing basic consumer data rights in federal privacy legislation empowers consumers to manage how others collect, use, and share their personal information. These data rights should include: the **right to be informed** about how organizations collection and use their personal data; the **right to be notified** about data breaches involving their personal data; the **right to consent** about the use of their personal data (opt-in consent for sensitive personal information in certain contexts; opt-out consent for most others); the **right to access** a copy of their personal information; the **right to delete** their personal information; the **right to rectify** incorrect their personal information; and the **right to port** a copy of their personal information. Creating these basic consumer data rights obligates organizations that collect and process personal data to respond to consumer requests.

Data minimization is the principle that organizations should collect and store the least amount of data possible about individuals to fulfill a specific purpose. If Congress establishes basic consumer data rights, then it would be unnecessary to create data minimization requirements because consumers already could learn how organizations use their personal information, opt out of data collection they do not support, and require that organizations that have collected their personal data delete it.

And data minimization does not come without cost. First, data minimization creates legal uncertainty for businesses because determining what data is "reasonably necessary" for a given purpose is subjective. This legal uncertainty discourages firms from investing in innovative uses of data because of increased regulatory risk. Second, minimizing the data organizations collect and store artificially limits how organizations can innovate with data. Consider a company

that provides direct-to-consumer genetic testing like 23andMe or Helix. Data minimization would say that these companies should throw out consumer genetic data after they run a test and only keep the results. But keeping the data allows them to do more analysis. For example, the company might discover later that there are additional genetic markers that they can test to give their customers more accurate results or new insights. Collecting data is expensive. Throwing data away, rather than reusing it, is unnecessarily wasteful—it's the data equivalent of drinking from single-use plastic bottles.

2. Your testimony calls for "preempting state and local privacy laws" in federal legislation. As you know, this has been a major topic of disagreement among stakeholders and advocates, which could be an obstacle to legislative progress. In your view, are there any possible middle grounds on the question of preemption? For example, might Congress leave more room for state and local laws on certain topics while leaving less room on other topics?

All Americans should have the same data privacy protections regardless of where they live, and companies should not be faced with 50 different sets of data privacy laws and regulations. A patchwork of state data privacy laws with varying definitions and requirements would create a complex regulatory minefield for businesses to navigate, especially if potential violations risk costly litigation. The goal of Congress should be to minimize unnecessary compliance costs for businesses so that they can concentrate their resources not on hiring more privacy lawyers to protect them from potential fines for non-compliance but on investments that will lead to more secure and privacy-preserving products and services.

Some stakeholders and advocates oppose state preemption because they want to ensure that if they do not get certain measures in a federal law, there is still a door open for them to pass those provisions in some states. For example, some stakeholders and advocates want to create a private right of action that would greatly benefit trial lawyers but do little for consumers. Others would tack on additional regulations for specific types of data, such as biometric data or children's personal data. Indeed, there are 50 state data breach laws, each slightly different, although they all share the same purpose. But these types of carve-out and variations raise costs for compliance, confuse consumers, and erode the benefits of creating a uniform federal law.

One way to achieve a middle ground on state preemption is to give state attorneys general more authority in enforcing future federal data privacy rules. While there should be one set of national rules, and one set of interpretation of those rules, state attorneys general should be allowed to bring cases against firms that break these rules and involve a substantial number of that state's residents. Allowing for broad enforcement capabilities will ensure that states can remain responsive to local needs. This type of enforcement would be especially beneficial if a federal data privacy law includes a 60 or 90-day cure period, wherein firms have a designated period to fix any alleged violation before further enforcement action occurs, because it would expedite oversight and compliance.

3. In recent years, both the legislative and executive branches have devoted increasing attention to fostering competition in online apps, services, and platforms. How does this goal interact with the protection of digital privacy? Can privacy and competition efforts conflict with one another -- for example, in requiring that a platform provide third parties with access to user data -- and if so, how might Congress balance these goals?

As Justice Louis Brandeis once wrote, privacy is the right to be left alone. Unfortunately, many of the proposed remedies to foster competition online involve requiring interoperability between various platforms that would undermine this notion of privacy. For example, interoperability requirements between competing social networks could make it harder, if not outright impossible, for these platforms to prevent harassment, spam, phishing attempts, and other unsolicited (and often unwelcome) messages—in essence making it harder for individuals to be left alone. The result of imposing interoperability requirements could be social networks where users are bombarded with robocalls and spam texts, much like many consumers experience on their mobile phone today, and platforms struggle to keep out malicious actors.

Moreover, interoperability requirements could force apps, services, and platforms to expose personal information they collect about their users to competitors. These competitors may not have sufficient safeguards to protect personal data. Moreover, there would likely be no restrictions to prevent these apps, services, and platforms from sharing data with a foreign competitor that may present an economic or national security threat to the United States.

Some stakeholders and advocates say that the presence or absence of data privacy measures in online apps and services reflects product quality. Moreover, they argue

that online apps and services that collect and use data, such as for targeted advertising, are necessarily indicative of poor quality and therefore the presence of these types of products is a sign of insufficient competition. But this critique ignores that consumers have different privacy preference and disregards the fact that consumers can often choose alternatives, including paying for online apps and services that offer additional privacy protections.

If Congress is concerned about privacy as a non-price factor in competition among online apps, services, and platforms it should address this concern by passing federal data privacy legislation. Congress should not use competition policy to address privacy concerns (or vice versa). While there may be important pro-competitive effects from some data privacy proposals, such as establishing a right to data portability, the primary rationale for those proposals is to maximize the value of personal data for consumers.

SUBMISSIONS FOR THE RECORD



**National Association of
Assistant United States Attorneys**
Safeguarding Justice for All Americans

Board of Directors

Steven B. Wasserman
President
(DC)

Adam E. Hanna
Vice President
(S.D. IL)

Mark Vincent
Treasurer
(UT)

David A. Marye
Secretary
(E.D. KY)

Kevan Cleary
(E.D. NY)

Karen Escobar
(E.D. CA)

Joseph Koehler
(AZ)

Clay West
(W.D. MI)

Executive Director
Robert O. Patterson

Washington Reps.
Jason Briefel
Natalia Castro

Counsel
Debra Roth

February 25, 2022

Chairperson Zoe Lofgren
House Committee on
House Administration
1309 Longworth House Office Bldg
Washington, DC 20515

Ranking Member Rodney Davis
House Committee on
House Administration
1309 Longworth House Office Bldg
Washington, DC 20515

**RE: NAAUSA Testimony for the House Administration Hearing on Big Data: Privacy
Risks and Needed Reforms in the Public and Private Sectors**

Dear Chairperson Lofgren, Ranking Member Davis, and Members of the Committee:

On behalf of the National Association of Assistant United States Attorneys (NAAUSA), representing the interests of the 6,300 Assistant U.S. Attorneys (AUSAs) working in the 93 U.S. Attorney Offices, I write you to express our perspective on privacy security issues impacting federal law enforcement, and particularly AUSAs.

On July 19, 2020, a disgruntled attorney targeted the home of U.S. District Court Judge Esther Salas. The assailant opened fire on Judge Salas' 20-year-old son, Daniel, who tragically died in the attack. Judge Salas' husband, Mark, was critically injured. This devastating case shed light onto concerns regarding a potential criminal's access to personal, private information on members of the law enforcement community and their families.

Unfortunately, it is not an isolated incident. The judges, federal prosecutors, and law enforcement officers who represent the front line and front face of our federal law enforcement system are constantly under threat of attack.

Data from the Department of Justice indicates that nearly 500 threats or inappropriate communications were levied against AUSAs in the last three years. Of these, 129 were death threats against AUSAs or their families. While the risk of a vengeful criminal attack is one many AUSAs dutifully take on in pursuit of justice for victims, our families should not be subject to these harms and reasonable steps must be taken to prevent these threats from actualizing.

Like many of the privacy issues discussed during this hearing, these privacy concerns transcend state lines. So, while several states have laws protecting private personal information about law enforcement, the lack of such a law at the federal level leaves dangerous privacy gaps.

The Senate Judiciary Committee has considered Daniel Anderl Judicial Security and Privacy Act of 2021 ([S. 2340](#)). This legislation, named in honor of U.S. District Judge Esther Salas' son, is a bipartisan effort to protect federal judges from violent criminals seeking revenge for the judge's role in the criminal justice system. This is an important Act that will undoubtedly make judges safer by protecting their personally identifiable information in public records and providing judicial security training.

While NAAUSA supports the focus on protecting federal judges, Congress must recognize that many members of the federal community face similar threats and security risks as federal judges. **We have urged lawmakers to amend the Daniel Aderl Judicial Security and Privacy Act of 2021 to include federal prosecutors so to extend the protections afforded to federal judges to federal prosecutors and all federal employees.**

Doxing, as it has been called, is becoming an increasingly common tool for criminal actors seeking revenge against the U.S. justice system in the internet age. Congress, States, and the Department of Justice must work quickly to prevent this violent trend from endangering the lives of more government employees and their families.

We should not wait until another member of the law enforcement community is attacked to take action to protect their class of coworkers.

Last Congress, NAAUSA endorsed [the Public Servant Protection Act](#) introduced by Senator Tom Cotton. This bill would have given all government employees, elected officials, and appointees at all levels (Federal, State, Local, and Tribal) the right to have their home addresses and phone numbers—or the home addresses and phone numbers of their immediate family members—removed from any publicly-displayed website. The bill also made it a criminal offense to post a government official or their immediate family member's home address or phone number online with the intent to cause physical harm. NAAUSA supported this bill particularly because of its protection for *all* federal employees rather than some.

To further improve this legislation, NAAUSA recommended the civil action penalty be increased to create a greater incentive for information to be quickly removed from the internet. For example, under the civil provision of [California Law 6254.21](#) the penalty includes a damages award to public official to a maximum of three times the actual damages but in no cases less than \$4,000.

Given the [increasing hostility](#) toward members of the law enforcement profession and federal employees generally, NAAUSA feels it is critical that Congress work to deter violent acts against all federal employees and their families.

NAAUSA applauds this Committee's interest in privacy issues. The lack of data security and the ease at which criminal actors can access highly personal information about law enforcement presents real dangers to federal officials. As this Committee continues considers ways to improve privacy protections, we urge you to consider protecting the private personal information of federal officials. The Daniel Aderl Judicial Security and Privacy Act of 2021 and the Public Servant Protection Act are great places to start.

NAAUSA also has robust data on state level reforms that may aid this Committee in understanding present models for addressing this issue on the federal level. Please do not hesitate to reach out to Natalia Castro (ncastro@shawbransford.com) if we can be of further assistance on this matter.

Respectfully,



Steven B. Wasserman
President

ZOE LOFGREN, CALIFORNIA
CHAIRPERSON
 MARY GAY SCANLON, PENNSYLVANIA
VICE CHAIRPERSON
 JAMIE RASKIN, MARYLAND
 G.K. BUTTERFIELD, NORTH CAROLINA
 PETE AGUILAR, CALIFORNIA
 TERESA LEGER FERNANDEZ, NEW MEXICO
 JAMIE FLEET
 STAFF DIRECTOR

One Hundred Seventeenth
 Congress of the United States
 House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
 1309 LONGWORTH HOUSE OFFICE BUILDING
 WASHINGTON, DC 20515-6157
 202-225-2061 | CHA.HOUSE.GOV

RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER
 BARRY LOUDERMILK, GEORGIA
 BRYAN STEIL, WISCONSIN
 TIM MONAHAN
 MINORITY STAFF DIRECTOR

June 22, 2021

The Honorable Zoe Lofgren
 Chairperson
 Committee on House Administration
 1309 Longworth House Office Building
 Washington, DC 20009

Chairperson Lofgren:

I write today to request that the Committee on House Administration hold oversight hearings regarding the current operations of the Library of Congress (LOC) and Smithsonian Institution. In May of this year, I requested operational status updates from each legislative branch entity to inform our committee's understanding of reopening progress and, ultimately, the legislative branch's service to the American people.

The findings were concerning. We found that 410 professional staff from the LOC's Congressional Research Service remain in telework, and 77 additional LOC employees have been on administrative leave for thirty pay periods – in which they remain to this day. At the Smithsonian Institution, 4,500 employees remain in telework, and only 25 percent of their workforce is estimated to be vaccinated. Additionally, concerning conversations are occurring regarding permanent timed-ticket reservation systems across all Smithsonian museums, limiting the public's access to American treasures well beyond the timeline of the recent pandemic.

Our nation is celebrating its victory over COVID-19. The *New York Times* reports that infection rates continue to decrease throughout the Washington, DC-area with cases per 100,000 averaging in single digits.¹ More importantly, every adult in the Washington, DC-area has had free access to receive both doses of a vaccine for well over a month. Beyond the beltway, the Centers for Disease Control and Prevention (CDC) reports that at least 64.5 percent of adults, nationwide, have at least one vaccination.² Theaters, office buildings, sports arenas, restaurants, and more have reopened. People across the country are returning to work and the same goes for Congress. The halls of the House and Senate office buildings are active once again, and there is no excuse for legislative branch support offices to not be fully operational or to continue to have employees on COVID-related administrative leave. I believe the same holds true for America's premier network of museums and research centers that fall under the umbrella of the Smithsonian Institution.

¹ <https://www.nytimes.com/interactive/2021/us/washington-district-of-columbia-covid-cases.html>

² <https://covid.cdc.gov/covid-data-tracker/#vaccinations>

The Honorable Zoe Lofgren
June 22, 2021
Page two

The lack of guidance provided for these entities has resulted in uneven policies, creating confusion and wasteful spending. For these reasons, I am requesting that our Committee begin conducting oversight hearings to fully grasp the operational status of the entities within our jurisdiction and, if needed, get their employees back to work.

I eagerly await your response as I am desperate to get this government and this country back to work.

Sincerely,

A handwritten signature in blue ink that reads "Rodney Davis". The signature is written in a cursive, flowing style.

Rodney Davis
Ranking Member
Committee on House Administration



February 15, 2022

The Honorable Zoe Lofgren
Chair
Committee on House Administration
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Rodney Davis
Ranking Member
Committee on House Administration
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairperson Lofgren, Ranking Member Davis, and members of the committee,

My name is Matthew Feeney. I am the director of the Cato Institute's project on emerging technologies. Tomorrow's hearing, titled "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors," is relevant to my research, which focuses on how new and emerging technologies affect our civil liberties. The private and public use of "Big Data" is a critical issue at a time when there is bipartisan concern about the role of prominent technology companies and their influence on our civic and family lives.

Today's most popular online services collect vast troves of information about their users. As former Google CEO Eric Schmidt once put it in 2010, "With your permission, you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."¹ While services such as Google and Facebook remain popular among Americans, their collection of personal information prompts an understandable sense of unease, not least because law enforcement agencies at the state, local, and federal level analyze "Big Data" while conducting surveillance. Unfortunately, the state of 4th Amendment jurisprudence leaves much to be desired.

Congress can make reforms to address "Big Data" concerns, but these reforms should be carefully tailored to ensure that Americans are protected from unreasonable searches and seizures by the government without hampering growth and innovation in America's technology sector.

¹ Nick Saint, "Google CEO: 'We Know Where You Are. We Know Where You've Been. We Can More Or Less Know What You're Thinking About.'" *Business Insider*, October 4, 2010, <https://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10>.

GOVERNMENT USE OF BIG DATA

In recent years, the most prominent examples of government use of Big Data for surveillance were those revealed by former National Security Agency contractor Edward Snowden.² Bookshelves worth of books and articles have been written about the revelations, and an extensive accounting of them would require many more pages. For the purposes of this statement, it is enough to note that the Snowden revelations unveiled the vast scale of government access to personal information, which had previously been unknown to the public.

More recently, reporting suggests that the Central Intelligence Agency (CIA) has been conducting mass surveillance on Americans, a sad reflection on the state of reform many lawmakers and civil libertarians hoped for in the wake of the Snowden revelations.³

Government use of Big Data is not reserved to intelligence agencies that cite national security concerns as justification for surveillance. Domestic agencies have also engaged in surveillance fueled by Big Data. The Department of Homeland Security (DHS) has exploited the “border exception” to the Fourth Amendment, for example, allowing officers to conduct warrantless searches of electronic devices at international border crossings. In 2014, Palantir Technologies secured a contract to build a vast intelligence system capable of collecting data on a subject’s “schooling, family relationships, employment information, phone records, immigration history, foreign exchange program status, personal connections, biometric traits, criminal records, and home and work addresses.”⁴

State, local, and federal law enforcement agencies use surveillance tools to monitor Americans. Such tools include social media snooping software, cell site simulators, and facial recognition technology.⁵

Facial recognition is one of the most widely discussed surveillance technologies cited by civil libertarians. More than 2,200 law enforcement agencies and private companies in

² Lawfare, “Snowden Revelations,” accessed February 14, 2022, <https://www.lawfareblog.com/snowden-revelations>.

³ Matthew Guariglia and Andrew Crocker, “We Need Answers About the CIA’s Mass Surveillance,” *Electronic Frontier Foundation*, February 11, 2022, <https://www.eff.org/deeplinks/2022/02/we-need-answers-about-cias-mass-surveillance>.

⁴ Spencer Woodman, “Palantir Provides the Engine for Donald Trump’s Deportation Machine,” *The Intercept*, March 2, 2017, <https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/>.

⁵ Brennan Center for Justice, “Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement Agencies,” November 17, 2021, <https://www.brennancenter.org/our-work/research-reports/third-party-vendors-social-media-monitoring-tools-law-enforcement>; American Civil Liberties Union, “Stingray Tracking Devices: Who’s Got Them?” November 2018, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them>.

twenty-seven countries have used Clearview AI, a controversial facial image search engine.⁶ Clearview AI scrapes billions of images from social media platforms such as Instagram, Facebook, and Twitter. Investigators can search this database, uploading photos of suspects in the hopes of confirming their identity.⁷

Government use of Big Data is not reserved to law enforcement and intelligence agencies. Local governments are increasingly looking to “Smart City” technology to improve infrastructure.⁸ Smarter infrastructure could result in fewer car crashes, less congested traffic, and more efficient public transport. Although not ostensibly related to mass surveillance, these initiatives have the potential to unveil intimate details. One of the best examples of how collection of personal transport data can reveal intimate details of private lives is a blog post (which has since been deleted) published by Uber detailing one-night sexual encounters among users.⁹

THE PRIVACY PARADOX

Any attempts at Big Data regulation or legislation will have to tackle the privacy paradox at the heart of debates surrounding data and privacy. On the one hand, Americans claim to care about their privacy, yet their behavior suggests otherwise. Amid complaints about “surveillance capitalism” we should keep in mind that Americans are keen users of services that collect information about them. Fortunately for those Americans more privacy-focused there are many services available that allow them to communicate and browse the web without revealing personal information.¹⁰

The Institute for Progress’ Alec Stapp summarized the Privacy Paradox well, writing:

“There is a paradox at the heart of how people treat privacy. They say they value privacy while their actions imply they don’t. In other words, their stated preferences contradict their revealed preferences. Is this just another example of cheap talk? Research from behavioral economics and related fields has shown that privacy valuations are highly context-dependent and subject to social-desirability bias and endowment effects.”¹¹

⁶ Ryan Mac, Caroline Haskins, and Logan McDonald, “Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, And The NBA,” *BuzzFeed News*, February 27, 2020, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

⁷ Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It,” *The New York Times*, November 2, 2021, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

⁸ Jonathan Woetzel et al., “Smart cities: Digital solutions for a more livable future,” *McKinsey & Company*, June 5, 2018, <https://www.mckinsey.com/business-functions/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future>.

⁹ Bradley Voytek, “Rides of Glory,” *#UberData* (blog), Uber, <https://web.archive.org/web/20140827195715/http://blog.uber.com/ridesofglory>.

¹⁰ End-to-end encrypted chat service Signal and the web browser TOR being among perhaps the most notable.

¹¹ Alec Stapp and Ryan Hagemann, “Regulatory Comment: Hearings on Competition and Consumer Protection in the 21st Century, The Intersection Between Privacy, Big Data, and Competition,” *Niskanen*

Stapp went on to provide examples from a number of surveys showing that although many people claim to value their privacy, they often value their personal information at a low cost.

That “privacy” is not an absolute value must be considered by those concerned about “Big Data.” Privacy is a condition people enjoy when they control information about themselves.¹² The age of social media has shown us the wide variety of ways in which people control such information. Some people like to post photos of their meals, themselves, or their romantic partners. Others would never post such content, choosing instead to volunteer personal information in political forums or e-commerce platforms. Others enjoy Amazon and YouTube recommendations based on viewing and purchasing histories. There is no one-size-fits-all approach to privacy. Fortunately, the market currently provides Americans of all privacy views a variety of social media platforms and communications tools.

Lawmakers considering regulation or legislation related to Big Data ought to be reassured by the fact that most Americans are aware that popular online services analyze their personal data and that alternatives are available to Americans concerned about their privacy. Contrary to what many lawmakers have been saying over the last few years, popular online communication and web browsing services are not monopolies.

REFORM

Those seeking to address concerns associated with Big Data should consider the following principles guiding reform:

1) Update legislation.

The Electronic Communications Privacy Act (ECPA), passed in 1986, has yet to undergo a comprehensive revision accounting for more than thirty years of technological changes. The law allows law enforcement to access a wide range of intimate content such as emails, social media chats, and texts more than six months old without a warrant.¹³ Congress should address the loopholes in ECPA that currently allow law enforcement to access troves of personal communications without a warrant.

Center, August 20, 2018, https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0027-152798.pdf.

¹² Jan Holvast, “History of Privacy,” (conference paper, IFIP Advances in Information and Communication Technology, 2008),

<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1037.5642&rep=rep1&type=pdf>.

¹³ Electronic Privacy Information Center, “Electronic Communications Privacy Act (ECPA),” accessed February 15, 2022, <https://epic.org/ecpa/>.

Congress should also improve upon Supreme Court precedent and impose a warrant requirement for searches of electronic devices at the border. Lawmakers from both parties have supported such legislation.¹⁴

2) Control, don't ban, facial recognition

More than half of American adults have images of their faces stored in databases that law enforcement officials can search while conducting facial recognition queries.¹⁵ This is in large part thanks to the fact that many state departments of motor vehicles allow law enforcement to search their databases of driver's license photos.¹⁶ The result is what Georgetown researchers have called the "Perpetual Lineup."¹⁷ Concerns about facial recognition have promoted calls for a ban on the technology.¹⁸ This is not the best approach.

Although facial recognition does pose a significant threat to civil liberties it is not without benefits. Facial recognition has the potential to ease queues at cinemas, grocery stores, and train stations. In addition, it can be used to enhance security and could be used to aid in searches for missing children or adults with dementia. Jettisoning these benefits is fortunately not necessary in order to protect civil liberties. As I have outlined before, there are policies that could ensure facial recognition is used by law enforcement in a narrow and transparent way that would not infringe on civil liberties.¹⁹ These policies include a ban on real-time identification, removing data related to law-abiding Americans from databases, and open source, accuracy, and transparency requirements.²⁰

3) Embrace transparency

A regrettable feature of modern American law enforcement is its lack of transparency. Too often, Americans learn about what surveillance devices their governments use from journalists rather than elected officials. Federal agencies should be required to regularly release information about 1) how often they ask technology firms for users' personal data, 2) what new surveillance tools its officers are using, and 3) how and when data related to closed cases are purged.

¹⁴ Protecting Data at the Border Act, S. 1606, 116th Cong. (2019).

¹⁵ Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-up: Unregulated Police Face Recognition in America," *Georgetown Law Center on Privacy and Technology*, October 18, 2016, <https://www.perpetuallineup.org>.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Fight for the Future, "Ban Facial Recognition," accessed February 14, 2021, <https://www.banfacialrecognition.com>.

¹⁹ Matthew Feeney, "Should Police Facial Recognition Be Banned?" *Cato at Liberty* (blog), Cato Institute, May 13, 2019, <https://www.cato.org/blog/should-police-facial-recognition-be-banned>.

²⁰ Ibid.

4) Resist calls for “data ownership”

It is not uncommon in discussion about “Big Data” to hear “data ownership” proposals that would grant a property right in personal data. Although perhaps at first glance attractive, such proposals are conceptually confused and are not necessary to protect privacy.

Data is very different from traditional property. A property right entails a “bundle” of other rights, such as the right to exclude and alter property. If you have a property right in a house you can exclude others from it and alter it. It is also clear who owns a home and other pieces of property. Data does not have these qualities. Data is not excludable in the same way as a house. My enjoyment of data is not affected if you use the same data or alter the data for yourself. Similarly, it is not clear how such a property right would be allocated. Does my birthdate contain data about me, my mother, or my father? Should property rights in marriage data be assigned to one spouse or both?

Most importantly, allowing for a property right in data is not necessary for privacy, as Center for Growth and Opportunity scholar Will Rinehart has explained:

“[A] property right in data isn’t needed to establish consumer privacy rights. For evidence of this fact, one only needs only to consult the current laws in the United States. The Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Children’s Online Privacy Protection Act (COPPA), and the California Consumer Privacy Act (CCPA), just to name a few, all protect privacy without creating property rights. As Stanford Law Professor Lothar Determann has said quite bluntly, ‘no one owns data’ because data are already ‘subject to a complex landscape of access rights and restrictions.’ Privacy regulation already defines certain kinds of entitlements to control and contract upon data. Adding a superordinate property right on top of these existing restrictions would make the entire enterprise all that more complicated and undermine current efforts to grant consumers control. If data property rights were implemented, for example, would an individual be able to limit critical information from being shared with credit rating agencies?”²¹

As lawmakers consider regulations and legislation they should be wary of the risks of regulatory capture. Market incumbent firms such as Microsoft, Google, and Facebook are well positioned to comply with whatever new regulations and legislation emerge

²¹ *Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation, Before the Committee on Banking, Housing, and Urban Affairs, 116th Cong. (2019)* (testimony of Will Rinehart, Director of Technology and Innovation Policy at the American Action Forum), <https://www.banking.senate.gov/imo/media/doc/Rinehart%20Testimony10-24-19.pdf>.

from Congress. History teaches us that these firms will invest in preparing for new regulation, and competition may suffer if regulations and legislation results in costs for market entrants. One of the best examples of this dynamic can be found in Google's preparation for the European Union's General Data Protection Regulation (GDPR), its flagship set of privacy regulations. Google reportedly spent hundreds of years worth of human time preparing for GDPR, a set of regulations that has benefitted the Silicon Valley giant:

"Google, for example, has seen some unique market benefits following the activation of GDPR in May 2018. From April to July of last year, Google's market share increased by 0.93% while most other adtech vendors in North America and Europe lost ground. The lowest rank of adtech companies — the top 150 to 100 — lost the most market share, a decline of 31.86% on average. Google was of course prepared for privacy regulation ahead of time, having spent "hundreds of years of human time" and, ostensibly, billions of dollars to shore up its defenses."²²

Lawmakers on this side of the Atlantic should be wary of repeating Europe's experience.

Thank you for giving your attention to these important issues. I would welcome the opportunity to discuss my thoughts further with you or your staff.

Yours,

Matthew Feeney
Director, Project on Emerging Technologies
Cato Institute

²² Alex Moazed, "How GDPR is Helping Big Tech and Hurting Competition," *Applico*, accessed February 14, 2022, <https://www.applico.com/blog/how-gdpr-is-helping-big-tech-and-hurting-the-competition/>.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA	:	
	:	
v.	:	Criminal Case No. 21-582 (CRC)
	:	
MICHAEL A. SUSSMANN,	:	
	:	
Defendant.	:	

**GOVERNMENT’S MOTION TO INQUIRE INTO POTENTIAL CONFLICTS OF
INTEREST**

1. The United States of America, by and through its attorney, Special Counsel John H. Durham, respectfully moves this Court to inquire into potential conflicts of interest arising from the representation of the defendant by his current counsel, Latham & Watkins LLP (“Latham”). The Government has discussed these matters with the defense and believes that any potential conflicts likely could be addressed with a knowing and voluntary waiver by the defendant upon consultation with conflict-free counsel as appropriate. The Government believes that any such waiver should be put on the record prior to trial. As set forth in further detail below, it is possible that conflicts of interest could arise from the fact that Latham and/or its employees (i) previously represented others in the Special Counsel’s investigation whose interests may conflict with those of the defendant, (ii) previously represented the defendant and his prior employer in connection with events that likely will be relevant at trial or at any sentencing, and (iii) maintained professional and/or personal relationships with individuals who could be witnesses in these proceedings. Accordingly, for the reasons set forth below, the government respectfully requests that the Court inquire into the potential conflicts of interest set forth herein. Defense counsel has advised that the defendant has

been apprised of these issues, understands that he has the right to consult independent counsel, and presently intends to waive any potential conflict of interest. In support of this Motion, the government represents the following:

FACTUAL BACKGROUND

2. The defendant is charged in a one-count indictment with making a materially false statement to the FBI, in violation of Title 18, United States Code, Section 1001 (the “Indictment”). As set forth in the Indictment, on Sept. 19, 2016 – less than two months before the 2016 U.S. Presidential election – the defendant, a lawyer at a large international law firm (“Law Firm-1”) that was then serving as counsel to the Clinton Campaign, met with the FBI General Counsel at FBI Headquarters in Washington, D.C. The defendant provided the FBI General Counsel with purported data and “white papers” that allegedly demonstrated a covert communications channel between the Trump Organization and a Russia-based bank (“Russian Bank-1”). The Indictment alleges that the defendant lied in that meeting, falsely stating to the General Counsel that he was not providing the allegations to the FBI on behalf of any client. In fact, the defendant had assembled and conveyed the allegations to the FBI on behalf of at least two specific clients, including (i) a technology executive (“Tech Executive-1”) at a U.S.-based Internet company (“Internet Company-1”), and (ii) the Clinton Campaign.

3. The defendant’s billing records reflect that the defendant repeatedly billed the Clinton Campaign for his work on the Russian Bank-1 allegations. In compiling and disseminating these allegations, the defendant and Tech Executive-1 also had met and communicated with another law partner at Law Firm-1 who was then serving as General Counsel to the Clinton Campaign (“Campaign Lawyer-1”).

4. The Indictment also alleges that, beginning in approximately July 2016, Tech Executive-1 had worked with the defendant, a U.S. investigative firm retained by Law Firm-1 on behalf of the Clinton Campaign, numerous cyber researchers, and employees at multiple Internet companies to assemble the purported data and white papers. In connection with these efforts, Tech Executive-1 exploited his access to non-public and/or proprietary Internet data. Tech Executive-1 also enlisted the assistance of researchers at a U.S.-based university who were receiving and analyzing large amounts of Internet data in connection with a pending federal government cybersecurity research contract. Tech Executive-1 tasked these researchers to mine Internet data to establish “an inference” and “narrative” tying then-candidate Trump to Russia. In doing so, Tech Executive-1 indicated that he was seeking to please certain “VIPs,” referring to individuals at Law Firm-1 and the Clinton Campaign.

5. The Government’s evidence at trial will also establish that among the Internet data Tech Executive-1 and his associates exploited was domain name system (“DNS”) Internet traffic pertaining to (i) a particular healthcare provider, (ii) Trump Tower, (iii) Donald Trump’s Central Park West apartment building, and (iv) the Executive Office of the President of the United States (“EOP”). (Tech Executive-1’s employer, Internet Company-1, had come to access and maintain dedicated servers for the EOP as part of a sensitive arrangement whereby it provided DNS resolution services to the EOP. Tech Executive-1 and his associates exploited this arrangement by mining the EOP’s DNS traffic and other data for the purpose of gathering derogatory information about Donald Trump.)

6. The Indictment further details that on February 9, 2017, the defendant provided an updated set of allegations – including the Russian Bank-1 data and additional allegations relating

to Trump – to a second agency of the U.S. government (“Agency-2”). The Government’s evidence at trial will establish that these additional allegations relied, in part, on the purported DNS traffic that Tech Executive-1 and others had assembled pertaining to Trump Tower, Donald Trump’s New York City apartment building, the EOP, and the aforementioned healthcare provider. In his meeting with Agency-2, the defendant provided data which he claimed reflected purportedly suspicious DNS lookups by these entities of internet protocol (“IP”) addresses affiliated with a Russian mobile phone provider (“Russian Phone Provider-1”). The defendant further claimed that these lookups demonstrated that Trump and/or his associates were using supposedly rare, Russian-made wireless phones in the vicinity of the White House and other locations. The Special Counsel’s Office has identified no support for these allegations. Indeed, more complete DNS data that the Special Counsel’s Office obtained from a company that assisted Tech Executive-1 in assembling these allegations reflects that such DNS lookups were far from rare in the United States. For example, the more complete data that Tech Executive-1 and his associates gathered – but did not provide to Agency-2 – reflected that between approximately 2014 and 2017, there were a total of more than 3 million lookups of Russian Phone-Provider-1 IP addresses that originated with U.S.-based IP addresses. Fewer than 1,000 of these lookups originated with IP addresses affiliated with Trump Tower. In addition, the more complete data assembled by Tech Executive-1 and his associates reflected that DNS lookups involving the EOP and Russian Phone Provider-1 began at least as early 2014 (*i.e.*, during the Obama administration and years before Trump took office) – another fact which the allegations omitted.

7. In his meeting with Agency-2 employees, the defendant also made a substantially similar false statement as he had made to the FBI General Counsel. In particular, the defendant

asserted that he was not representing a particular client in conveying the above allegations. In truth and in fact, the defendant was representing Tech Executive-1 – a fact the defendant subsequently acknowledged under oath in December 2017 testimony before Congress (without identifying the client by name).

APPLICABLE LAW

8. The Sixth Amendment guarantees that “[i]n all criminal prosecutions, the accused shall ... have the Assistance of Counsel for his defense.” U.S. Const. Amend. VI. A defendant’s Sixth Amendment right includes the “right to representation that is free from conflicts of interest,” *Wood v. Georgia*, 450 U.S. 261, 271 (1981), but also carries a “presumption in favor of counsel of choice,” *Wheat v. United States*, 486 U.S. 153, 160 (1988). At the same time, a criminal defendant’s right to retain counsel of his choice is not absolute. The “essential aim” of the Sixth Amendment “is to guarantee an effective advocate for each criminal defendant rather than to ensure that a defendant will inexorably be represented by the lawyer whom he prefers.” *Wheat*, 486 U.S. at 159. Thus, even if a defendant waives the right to conflict-free representation, the presumption in favor of defendant’s counsel of choice “may be overcome not only by a demonstration of actual conflict but also by a showing of a serious potential for conflict.” *Wheat*, 486 U.S. at 163–64.

9. As the D.C. Circuit explained in *United States v. Lopesierra-Gutierrez*, 708 F.3d 193, 199–200 (D.C. Cir. 2013), “a defendant’s counsel-of-choice right may sometimes be trumped by a conflict of interest.” This is because “where a defendant’s chosen counsel suffers from a conflict of interest, . . . the court’s own institutional interests” are implicated. *Id.* Guaranteeing conflict-free counsel protects not just defendants’ rights, but also the “[f]ederal courts[’] ... independent interest in ensuring that criminal trials are conducted within the ethical standards of

the [legal] profession and that legal proceedings appear fair to all who observe them.” *Id.* (alterations in original) (quoting *Wheat*, 486 U.S. at 161).

10. Since the Court has an independent interest in investigating potential conflicts, *see Wheat*, 486 U.S. at 161, the Court retains “substantial latitude in refusing waivers of conflicts of interest not only in those rare cases where an actual conflict may be demonstrated before trial, but in the more common cases where a potential for conflict exists which may or may not burgeon into an actual conflict as the trial progresses.” *Id.* at 163. Accordingly, “[i]f in the context of a particular case the district court believes a conflict is intolerable, it may decline to accept a defendant’s waiver.” *Lopesierra-Gutierrez*, 708 F.3d at 202. “In making this determination, a court balances the defendant’s right to choose his representative against both the defendant’s countervailing right to conflict-free representation and the court’s independent interest in the integrity of criminal proceedings.” *Id.* at 200 (emphasis in original). The key inquiry in this analysis is the “nature and extent of the conflict.” *Id.*

DISCUSSION

11. The Government respectfully requests that the Court inquire concerning the following issues that may give rise to potential conflicts of interest with regard to Latham’s current representation of the defendant:

I. Latham’s Prior Representations in the Special Counsel’s Investigation

A. Latham’s Prior Representation of Law Firm-1 and Campaign Lawyer-1 in This Investigation

12. From approximately July 2020 through approximately July 2021, Latham represented three separate clients – the defendant, Law Firm-1, and Campaign Lawyer-1 – in

connection with the Special Counsel's investigation.¹ As part of its representations, Latham communicated and met with the Special Counsel's Office and other DOJ officials on behalf of each of these clients. As noted above, the Indictment alleges that Tech Executive-1 conferred and consulted with both the defendant and Campaign Lawyer-1 on multiple occasions in connection with the Russian Bank-1 allegations. As a result, the Government expects that testimony at trial will address factual issues concerning, among other things, (i) the extent to which the defendant did or did not inform Campaign Lawyer-1 and Law Firm-1 that he was billing work on the Russian Bank-1 allegations to the Clinton Campaign, (ii) the extent to which the defendant did or did not inform or receive instructions from Campaign Lawyer-1 and Law Firm-1 regarding his billing of the Clinton Campaign and his meeting with the FBI General Counsel, and (iii) the defendant's potential motives to mislead the FBI concerning whether he was working with or on behalf of the Clinton Campaign, Campaign Lawyer-1, and Tech Executive-1. In each of these areas, the defendant's interests may diverge from those of Campaign Lawyer-1 and Law Firm-1. In addition, to the extent that the defendant's factual accounts might differ from those of Campaign Lawyer-1 and Law Firm-1 on these issues, Latham may already have gained privileged insights to any such differences from their prior, confidential attorney-client communications. *Cf. United States v. Gotti*, 9 F. Supp. 2d 320, 323–25 (S.D.N.Y. 1998) (“attorney-client relationship with the witness or co-defendant gave rise to continuing obligations of loyalty and confidentiality that may be breached when the confidences are required to be exploited in, for example, cross examining [a] former

¹ One of the Latham attorneys who represented the defendant during this time period is now serving at the U.S. Department of Justice. It is the understanding of the Special Counsel's Office that this attorney expeditiously and appropriately recused himself from any involvement in the Special Counsel's investigation and these proceedings.

client”); *cf. also United States v. Weaver*, 265 F.3d 1]074, 1075–77 (D.C. Cir. 2001) (holding that counsel’s representation of a client and a potential witness against the client created a conflict of interest).

13. Moreover, it is possible that the defendant, having recently resigned from his partnership at Law Firm-1, is currently or will become in an adversarial posture with his former employer. Latham – through its prior representation of Law Firm-1 – likely possesses confidential knowledge about Law Firm-1’s role in, and views concerning, the defendant’s past activities. Accordingly, the Government believes that potential conflicts of interest may exist or arise from Latham’s prior representations of Campaign Lawyer-1 and Law Firm-1 in this investigation.

B. Law Firm-1’s Representation of the Clinton Campaign and Another Political Organization

14. Potential conflicts of interest might also arise from the fact that during the time period when Latham represented all three of the aforementioned clients, one of those clients, Law Firm-1, was representing both the Clinton Campaign and a related political organization (“Political Organization-1”) in the Special Counsel’s investigation. Law Firm-1’s representations of those clients began in approximately May 2021 and ended in approximately July 2021. The Government believes that Law Firm-1’s prior representations of these entities may give rise to potential conflicts of interest because it is possible that Law Firm-1 shared confidential facts and/or communications concerning its representation of those clients with its then-counsel, Latham. In addition, to the extent the Government offers documents and other evidence at trial that it obtained from the Clinton Campaign and/or Political Organization-1, Latham’s duties to its former client (Law Firm-1) might cause its interests to diverge from those of the defendant in connection with such evidence and/or the cross examination of witnesses. Accordingly, the Government respectfully requests that the

Court inquire into any potential conflicts, including an examination of whether Law Firm-1's own representations of the Clinton Campaign and Political Organization-1 may contribute to or amplify such conflicts. *Gotti*, 9 F Supp. 2d at 323-25.

II. Latham's Other Representations in Related Matters

15. In addition to the above representations, Latham also has represented the defendant, Law Firm-1, and Campaign Lawyer-1 in other matters that predated the existence of the Special Counsel's investigation but which are likely relevant to these proceedings. In particular, the Government is aware of the following:

A. Latham's Representation of the Defendant in his December 2017 Congressional Testimony

16. Latham served as counsel to the defendant and Law Firm-1 in connection with the defendant's December 2017 testimony before the House Permanent Subcommittee on Intelligence. That testimony addressed the Russian Bank-1 allegations and other matters. At numerous times during the defendant's testimony, attorneys from Latham interjected to clarify and/or address issues relating to attorney-client privilege and other topics.² In his testimony, the defendant acknowledged bringing the Russian Bank-1 allegations to the FBI General Counsel and to Agency-2 on behalf of a specific client, namely, Tech Executive-1 (whom the defendant did not identify by name). The Government expects to offer this testimony at trial to prove that the defendant knowingly and intentionally lied when he stated to the FBI General Counsel in September 2016 that he was *not* acting on behalf of "any client." The Government also may seek to establish that the defendant's Congressional testimony itself was knowingly and intentionally misleading insofar as it failed to

² Both of the Latham attorneys who were present for the defendant's testimony (one of whom is the Department of Justice employee referenced above) have since left the firm.

disclose that the defendant billed work on the Russian Bank-1 allegations to the Clinton Campaign. Because Latham attorneys played a role in, and were witnesses to, this testimony and related conversations, it is possible that their past advice might give rise to a potential conflict of interest. For example, it is possible that motion practice surrounding the admissibility of this testimony may require consideration of issues such as the appropriate boundaries of the attorney-client privilege, the potential waiver of such privilege by the defendant or Tech Executive-1 and the Clinton Campaign, and/or the potential applicability of an advice of counsel defense. Because Latham attorneys witnessed the defendant's testimony and advised both the defendant and his employer in connection therewith, it is possible that conflicts of interest would arise in connection with these matters. *Gotti*, 9 F. Supp. 2d at 324 ("An attorney may be disqualified if he has first-hand knowledge of events that may be part of the government's proof at trial.")

B. Latham's Advice to Law Firm-1 in Connection with Public Statements in 2018

17. In 2018, Latham also advised Law Firm-1 concerning the drafting and issuance of statements to the media that Law Firm-1 made concerning the defendant's October 2016 meeting with the FBI General Counsel. Those statements – which the defendant appears to have reviewed or assisted in drafting – were at least partially inaccurate and/or misleading. The Government therefore may seek to offer these statements at trial pursuant to Rule 404(b) or other provisions of law. The two statements are, in pertinent part, as follows:

- On or about October 12, 2018, Law Firm-1 issued a statement to multiple media outlets in which the firm stated, in part: "When Sussmann met with [the FBI General Counsel] on behalf of a client, it was not connected to the firm's representation of the Hillary Clinton Campaign, the DNC or any Political Law Group client."

- On or about October 18, 2018, the then-Managing Partner of Law Firm-1 wrote a letter to the editor of a major newspaper in which he asserted, in part, “Mr. Sussmann’s meeting with the FBI General Counsel James Baker was on behalf of a client with no connections to either the Clinton campaign, the DNC or any other Political Law Group client.”

Privilege logs and redacted emails obtained from Law Firm-1 in this investigation reflect that in the days before the issuance of these statements, Latham attorneys sent, received, and/or were copied on correspondence relating to the drafting and dissemination of the statements. (Much of the substance of those emails was redacted and withheld from the Special Counsel’s Office pursuant to Law Firm-1’s assertion of attorney-client privilege and attorney work product protections). Because the defendant was aware of and/or reviewed these media statements, the Government may seek to offer them as evidence pursuant to Rule 404(b) or other provisions of law to establish that the defendant sought to conceal the Clinton Campaign’s ties to the Russian Bank-1 allegations from the FBI and others.³ Latham’s advice concerning these statements therefore may become at issue in motions *in limine*, trial testimony, or other aspects of these proceedings. Accordingly, Latham may encounter potential conflicts of interest in advising the defendant concerning past events in which Latham played a significant role.

³ According to counsel for Law Firm-1, the attorneys at Law Firm-1 and Latham who participated in drafting and/or reviewing these statements were unaware at the time that the defendant had billed work on the Russian Bank-1 allegations to the Clinton Campaign.

III. Defense Counsel's Prior Interactions with Witnesses or Potential Witnesses

18. Based on its review of documents in its investigation and other information, the Special Counsel's Office also has learned that one of the members of the defendant's current defense team ("Defense Team Member-1") previously worked as Special Counsel to the then-FBI Director from 2013 to 2014. In connection with that work, Defense Team Member-1 developed professional and/or personal relationships with several individuals who later were involved with and/or knowledgeable of the FBI's investigation of the Russian Bank-1 allegations. For example, Defense Team Member-1 appears to have developed a professional relationship with the former FBI General Counsel to whom the defendant made his alleged false statement and who will likely be a central witness at trial.⁴ While it is unlikely that these past interactions and activities will give rise to an actual conflict of interest, the Government respectfully requests in an abundance of caution that the Court inquire with the defense concerning whether Defense Team Member-1's relationships with persons and entities who might be witnesses in this case could give rise to a potential conflict or appearance issue and, if so, whether the defendant waives any such conflict. *See Lyle v. Artuz*, No 03-CV-5155 (CBA), 2006 WL 1517750 at *20 (E.D.N.Y. May 31, 2006)

⁴ Following his employment at the FBI, Defense Team Member-1 worked from 2014 to early 2017 as an attorney in the EOP which, as noted above, was involved in certain factual issues that the Government expects will be relevant at trial and any sentencing proceedings. Latham has represented to the Government that while employed at the EOP, Defense Team Member-1 had no role in the aforementioned events or arrangements involving Tech Executive-1, Internet Company-1, and/or allegations involving the purported use of Russian-made phones. The Government similarly has not seen evidence to suggest that Defense Team Member-1 had any role in, or direct knowledge of, the Russian Bank-1 allegations or the FBI's ensuing investigation.

(examining whether defense counsel's relationship with a trial witness gave rise to a conflict of interest).

CONCLUSION

For the foregoing reasons, the Court should inquire regarding the potential conflicts of interest set forth above.

Respectfully submitted,

JOHN H. DURHAM
Special Counsel

By:

/s/ Andrew J. DeFilippis
Jonathan E. Algor
Assistant Special Counsel
jonathan.algor@usdoj.gov

Andrew J. DeFilippis
Assistant Special Counsel
andrew.defilippis@usdoj.gov

Michael T. Keilty
Assistant Special Counsel
michael.keilty@usdoj.gov

Clinton campaign paid to 'infiltrate' Trump Tower, White House servers to link Trump to Russia, Durham finds

'Tech Executive-1 and his associates exploited this arrangement by mining the EOP's DNS traffic and other data for the purpose of gathering derogatory information about Donald Trump.'

[Brooke Singman](#) 3 days ago

[Two men indicted by Durham will go on trial in 2022](#)

Former Federal Prosecutor James Trusty details what to expect in 2022 as two men have been indicted as a result of the Durham probe into the roots of the Trump-Russia investigation

NEWYou can now listen to Fox News articles!

First on Fox: Lawyers for the [Clinton](#) campaign paid a technology company to "infiltrate" servers belonging to Trump Tower, and later the [White House](#), in order to establish an "inference" and "narrative" to bring to government agencies linking [Donald Trump](#) to [Russia](#), a filing from Special Counsel [John Durham](#) found.

Durham filed a motion on Feb. 11 focused on potential conflicts of interest related to the representation of former Clinton campaign lawyer Michael Sussmann, who has been charged with making a false

statement to a federal agent. Sussmann has pleaded not guilty.

The indictment against Sussmann, says he told then-FBI General Counsel James Baker in September 2016, less than two months before the 2016 presidential election, that he was not doing work "for any client" when he requested and held a meeting in which he presented "purported data and 'white papers' that allegedly demonstrated a covert communications channel" between the Trump Organization and Alfa Bank, which has ties to the Kremlin.

DECLASSIFIED TRUMP-RUSSIA PROBE DOCS TO DATE: WHAT TO KNOW

But Durham's filing on Feb. 11, in a section titled "Factual Background," reveals that Sussmann "had assembled and conveyed the allegations to the FBI on behalf of at least two specific clients, including a technology executive (Tech Executive 1) at a U.S.-based internet company (Internet Company 1) and the Clinton campaign."

Durham's filing said Sussmann's "billing records reflect" that he "repeatedly billed the Clinton Campaign for his work on the Russian Bank-1 allegations."



Special Counsel John H. Durham

The filing revealed that Sussmann and the Tech Executive had met and communicated with another law partner, who was serving as General Counsel to the Clinton campaign. Sources told Fox News that lawyer is Marc Elias, who worked at the law firm Perkins Coie.

Durham's filing states that in July 2016, the tech executive worked with Sussmann, a U.S. investigative firm retained by Law Firm 1 on behalf of the Clinton campaign, numerous cyber researchers and employees at multiple internet companies to "assemble the purported data and white papers."

"In connection with these efforts, Tech Executive-1 exploited his access to non-public and/or proprietary Internet data," the filing states. "Tech Executive-1 also enlisted the assistance of researchers at a U.S.-based university who were receiving and analyzing large amounts of Internet data in connection with a pending federal government

cybersecurity research contract."

"Tech Executive-1 tasked these researchers to mine Internet data to establish 'an inference' and 'narrative' tying then-candidate Trump to Russia," Durham states. "In doing so, Tech Executive-1 indicated that he was seeking to please certain 'VIPs,' referring to individuals at Law Firm-1 and the Clinton campaign."



Former U.S. President Bill Clinton and First Lady Hillary Clinton arrive for the Presidential Inauguration of Trump at the U.S. Capitol in Washington, D.C., U.S., January 20, 2017. (REUTERS/Saul Loeb/Pool)

Durham also writes that during Sussmann's trial, the government will establish that among the Internet data Tech Executive-1 and his associates exploited was domain name system (DNS) internet traffic pertaining to "(i) a particular healthcare provider, (ii) Trump Tower, (iii) Donald Trump's Central Park West apartment building, and (iv) the Executive Office of the President of the United States (EOP)."

[SPECIAL COUNSEL JOHN DURHAM 'STILL IN ACTION,' GARLAND SAYS](#)

Durham states that the internet company that Tech Executive-1 worked for "had come to access and maintain dedicated servers" for the Executive Office of the President as "part of a sensitive arrangement whereby it provided DNS resolution services to the EOP."

"Tech Executive-1 and his associates exploited this arrangement by mining the EOP's DNS traffic and other data for the purpose of gathering derogatory information about Donald Trump," Durham states.

The filing also reveals that Sussmann provided "an updated set of allegations" including the Russian bank data, and additional allegations relating to Trump "to a second agency of the U.S. government" in 2017.

Durham says the allegations "relied, in part, on the purported DNS traffic" that Tech Executive-1 and others "had assembled pertaining to Trump Tower, Donald Trump's New York City apartment building, the EOP, and the aforementioned healthcare provider."

In Sussmann's meeting with the second U.S. government agency, Durham says he "provided data which he claimed reflected purportedly suspicious DNS lookups by these entities of internet protocol (IP) addresses affiliated with a Russian mobile phone provider," and claimed that the lookups "demonstrated Trump and/or his associates were using supposedly rare, Russian-made wireless phones in the vicinity of the White House and other locations."



Pedestrians pass the Trump Tower building, Tuesday, July 7, 2020, in New York. (AP Photo/Frank Franklin II)

"The Special Counsel's Office has identified no support for these allegations," Durham wrote, adding that the "lookups were far from rare in the United States."

"For example, the more complete data that Tech Executive-1 and his associates gathered--but did not provide to Agency 2--reflected that between approximately 2014 and 2017, there were a total of more than 3 million lookups of Russian Phone-Prover 1 IP addresses that originated with U.S.-based IP addresses," Durham wrote. "Fewer than 1,000 of these lookups originated with IP addresses affiliated with Trump Tower."

Durham added that data collected by Tech Executive-1 also found that lookups began as early as 2014, during the Obama administration and years before Trump took office, which he said, is "another fact which the allegations omitted."

**DURHAM TARGETS CLINTON CAMPAIGN LAW FIRM IN FRESH
ROUND OF SUBPOENAS**

"In his meeting with Agency-2 employees, the defendant also made a substantially similar false statement as he made to the FBI General Counsel," Durham wrote. "In particular, the defendant asserted that he was not representing a particular client in conveying the above allegations."

"In truth and in fact, the defendant was representing Tech Executive-1--a fact the defendant subsequently acknowledged under oath in December 2017 testimony before Congress, without identifying the client by name," Durham wrote.

Former President Trump reacted to the filing on Saturday evening, saying Durham's filing "provides indisputable evidence that my campaign and presidency were spied on by operatives paid by the Hillary Clinton Campaign in an effort to develop a completely fabricated connection to Russia."

"This is a scandal far greater in scope and magnitude than Watergate and those who were involved in and knew about this spying operation should be subject to criminal prosecution," Trump said. "In a stronger period of time in our country, this crime would have been punishable by death."

Trump added: "In addition, reparations should be paid to those in our country who have been damaged by this."

Former chief investigator of the Trump-Russia probe for the House Intelligence Committee under then-Rep. Devin Nunes, R-Calif., Kash Patel, said the filing "definitively shows that the Hillary Clinton

campaign directly funded and ordered its lawyers at Perkins Coie to orchestrate a criminal enterprise to fabricate a connection between President Trump and Russia."

"Per Durham, this arrangement was put in motion in July of 2016, meaning the Hillary Clinton campaign and her lawyers masterminded the most intricate and coordinated conspiracy against Trump when he was both a candidate and later President of the United States while simultaneously perpetuating the bogus Steele Dossier hoax," Patel told Fox News, adding that the lawyers worked to "infiltrate" Trump Tower and White House servers.

The anti-Trump dossier, authored by ex-British intelligence officer Christopher Steele, commissioned by opposition research firm Fusion GPS, was funded by the Democratic National Committee and Hillary Clinton's campaign through Elia's law firm, Perkins Coie.

Patel added that Sussmann relayed the "false narrative" to U.S. government agencies "in the hopes of having them launch investigations of President Trump."

Sussmann's indictment is the second prosecution to come out of Durham's probe.



Sussman pic: Perkins Coie (Perkins Coie)

In November 2021, Durham also charged [Russian](#) national Igor Danchenko of making false statements. Danchenko, who pleaded not guilty, is accused of lying about the source of information that he provided to Christopher Steele for his "dossier" on Trump.

In 2020, Durham charged former FBI lawyer Kevin Clinesmith with making a false statement – the first criminal case arising from his probe. Clinesmith was referred for potential prosecution by the [Justice Department's](#) inspector general's office, which conducted its own review of the Russia investigation.

Specifically, the inspector general accused Clinesmith, though not by name, of altering an email about Page to say that he was "not a source" for another government agency. Page has said he was a source for the CIA. The DOJ relied on that assertion as it submitted a third and final renewal application in 2017 to eavesdrop on Trump campaign aide

Carter Page under the Foreign Intelligence Surveillance Act (FISA).

Former Attorney General Bill Barr appointed Durham, then the U.S. attorney from Connecticut, in 2019 to investigate the origins of the FBI's original Russia probe, or Crossfire Hurricane, which began in July 2016, through the appointment of Special Counsel Robert Mueller in May 2017 shortly after Mueller completed his years long investigation into whether Trump's campaign colluded or coordinated with the Russians to influence the 2016 presidential election.

Mueller's investigation found no evidence of illegal or criminal coordination between Trump or the Trump campaign and Russia in 2016.

Barr, in December 2020, before leaving the Trump administration, tapped Durham as special counsel to continue his investigation through the Biden administration.

[GET THE FOX NEWS APP HERE](#)

In the scope order, Barr stated that Durham "is authorized to investigate whether any federal official, employee, or any other person or entity violated the law in connection with the intelligence, counter-intelligence, or law-enforcement activities directed at the 2016 presidential campaigns, individuals associated with those campaigns, and individuals associated with the administration of President Donald J. Trump, including but not limited to Crossfire Hurricane and the investigation of Special Counsel Robert S. Mueller, III."

Under U.S. code, the special counsel would produce a "confidential report" and is ordered to "submit to the Attorney General a final report, and such interim reports as he deems appropriate in a form that will

permit public dissemination."

Brooke Singman is a Politics Reporter for Fox News. You can reach her at Brooke.Singman@Fox.com or @BrookeSingman on Twitter.

