CONSUMER PERSPECTIVES: POLICY PRINCIPLES FOR A FEDERAL DATA PRIVACY FRAMEWORK

HEARING
BEFORE THE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE
ONE HUNDRED SIXTEENTH CONGRESS
FIRST SESSION
MAY 1, 2019

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

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

<table>
<thead>
<tr>
<th>Hearing held on May 1, 2019</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of Senator Wicker</td>
<td>1</td>
</tr>
<tr>
<td>Statement of Senator Cantwell</td>
<td>3</td>
</tr>
<tr>
<td>Statement of Senator Blunt</td>
<td>59</td>
</tr>
<tr>
<td>Statement of Senator Schatz</td>
<td>61</td>
</tr>
<tr>
<td>Statement of Senator Fischer</td>
<td>63</td>
</tr>
<tr>
<td>Statement of Senator Tester</td>
<td>65</td>
</tr>
<tr>
<td>Statement of Senator Blackburn</td>
<td>67</td>
</tr>
<tr>
<td>Statement of Senator Peters</td>
<td>68</td>
</tr>
<tr>
<td>Statement of Senator Thune</td>
<td>70</td>
</tr>
<tr>
<td>Statement of Senator Markey</td>
<td>72</td>
</tr>
<tr>
<td>Statement of Senator Moran</td>
<td>75</td>
</tr>
<tr>
<td>Statement of Senator Rosen</td>
<td>76</td>
</tr>
<tr>
<td>Statement of Senator Blumenthal</td>
<td>78</td>
</tr>
<tr>
<td>Statement of Senator Sinema</td>
<td>80</td>
</tr>
<tr>
<td>Statement of Senator Sullivan</td>
<td>81</td>
</tr>
<tr>
<td>Statement of Senator Cruz</td>
<td>83</td>
</tr>
</tbody>
</table>

### WITNESSES

| Helen Dixon, Commissioner, Data Protection Commission of Ireland | 5 |
| Jules Polonetsky, Chief Executive Officer, Future of Privacy Forum | 12 |
| James P. Steyer, Chief Executive Officer and Founder, Common Sense Media | 26 |
| Neema Singh Guliani, Senior Legislative Counsel, Washington Legislative Office, American Civil Liberties Union | 31 |

### APPENDIX

<table>
<thead>
<tr>
<th>Response to written questions submitted by Hon. Jerry Moran to:</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helen Dixon</td>
<td>87</td>
</tr>
<tr>
<td>Jules Polonetsky</td>
<td>88</td>
</tr>
<tr>
<td>Neema Singh Guliani</td>
<td>90</td>
</tr>
</tbody>
</table>
CONSUMER PERSPECTIVES:
POLICY PRINCIPLES FOR A FEDERAL
DATA PRIVACY FRAMEWORK

WEDNESDAY, MAY 1, 2019

U.S. Senate,
Committee on Commerce, Science, and Transportation,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m. in room SD-G50, Dirksen Senate Office Building, Hon. Roger Wicker, Chairman of the Committee, presiding.


OPENING STATEMENT OF HON. ROGER WICKER,
U.S. Senator from Mississippi

The CHAIRMAN. Good morning.

Today, the Committee gathers for another hearing on consumer data privacy.

I am glad to convene this hearing with my colleague, Ranking Member Cantwell, and I welcome our witnesses and thank them for appearing today: Ms. Helen Dixon, Ireland’s Data Protection Commissioner; Mr. Jules Polonetsky, CEO of the Future of Privacy Forum; Mr. Jim Steyer, CEO and founder of Common Sense Media; and Ms. Neema Singh Guliani, Senior Legislative Counsel for the American Civil Liberties Union. Welcome to all of you.

Consumers are the bedrock of our economy. Through the consumption of goods and services, consumers drive economic activity, power job creation, and create opportunities for innovation and economic advancement in the United States and around the world.

To foster relationships with consumers, businesses have historically collected and used information about their patrons. The collection of data about consumers’ likes, dislikes, and commercial interests has ultimately served to benefit consumers in the form of more customized products and services and more choices at reduced costs.

Consumer data has tremendous societal benefits as well. In a world of “big data” where physical objects and processes are digitized, there is an increased volume of consumer data flowing throughout the economy. This data is advancing entire economic sectors such as health care, transportation, and manufacturing. Data enables these sectors to improve their operations, target re-
sources and services to underserved populations and increase their competitiveness.

The consumer benefits of a data-driven economy are undeniable. These benefits are what fuel the vibrancy and dynamism of today’s Internet marketplace. Despite these benefits, however, near daily reports of data breaches and data misuse underscore how privacy risks within the data-driven economy can no longer be ignored.

The increased prevalence of privacy violations threatens to undermine consumers’ trust in the Internet marketplace. This could reduce consumer engagement and jeopardize the long-term sustainability and prosperity of the digital economy.

Consumer trust is essential. To maintain trust, a strong, uniform Federal data privacy framework should adequately protect consumer data from misuse and other unwanted data collection and processing. When engaging in commerce, consumers should rightly expect that their data will be protected.

So today, I hope our witnesses will address how a Federal privacy law should provide consumers with more transparency, choice, and control over their information to prevent harmful data practices that reduce consumer confidence and stifle economic engagement.

To provide consumers with more choice and control over their information, both the European Union’s General Data Protection Regulation and the California Consumer Privacy Act provide consumers with certain privacy rights. Some of these rights include the right to be informed or the right to know; the right of access; the right to erasure or deletion; the right to data portability; and the right to nondiscrimination, among others.

I hope our witnesses will address how to provide these types of rights within a United States Federal framework without unintentionally requiring companies to collect and retain more consumer data. Provisioning certain privacy rights to individuals without minimum controls may have the opposite effect of increasing privacy risks for consumers.

In developing a Federal privacy law, the existing notice and choice paradigm also has come under scrutiny. Under notice and choice, businesses provide consumers with notice typically through a lengthy and wordy privacy policy about their data collection and processing practices. Consumers are then expected to make a “take it or leave it” choice about whether or not to purchase or use a product or service. But is this really a choice?

I hope our witnesses will address how to ensure that consumers have access to simplified notices that offer meaningful choices about what information an organization collects about them instead of a lengthy and confusing privacy notice or terms of use that are often written in legalese and bury an organization’s data collection activities.

I also hope witnesses will speak to ways in which Congress can provide additional tools and resources for consumers to make informed privacy decisions about the products and services they choose to use both online and offline.

Fundamental to providing truly meaningful privacy protections for consumers is a strong, consistent Federal law. This is critical to reducing consumer confusion about their privacy rights and en-
suring that consumers can maintain the same privacy expectations across the country.

I look forward to a thoughtful discussion on these issues. And again, welcome to all of our witnesses.

I now recognize my good friend and Ranking Member, Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman.

And thank you to the witnesses for being here today on this important hearing about how to develop a Federal data privacy framework. It is essential that we give a front row seat to the consumer advocate perspective, and that is what today’s conversation does.

When the dust settles after a data breach or a misuse of data, consumers are the ones who are left harmed and disillusioned. In the two months since our last Full Committee hearing on privacy, consumer data has continued to be mishandled. It is clear that companies have not adequately learned from past failures, and at the expense of consumers, we are seeing that self-regulation is insufficient.

Just days ago, cybersecurity researchers revealed the existence of a massive cloud data breach left wide open and unprotected, containing addresses, full names, dates of birth, income, marital status on more than 80 million U.S. households. This blatant disregard for security and privacy risks makes it clear why we are here today.

Microsoft recently admitted that an undisclosed number of consumer Web e-mail accounts were compromised. We learned more about privacy lapses on Facebook and two more third party Facebook apps exposed data on Facebook users revealing over 540 million records including comments, likes, account names, and Facebook IDs.

So, Mr. Chairman, how do we create a culture of data security that protects consumers and allows commerce to continue to grow?

Consumers continue to be bombarded by threats to their privacy. Cybersecurity adversaries become more sophisticated and more organized day by day, and we really need to understand privacy on a continuum of data security. We need to make a more proactive approach to cybersecurity and make sure that we are continuing to protect consumers.

This becomes especially important in the age of Internet of Things. Yesterday, the Security Subcommittee considered this issue at length. Billions of devices collecting data about consumers at all times means there are billions of entry points and large surface areas for cyber attack. We learned more about new botnet attacks and now weaknesses almost daily.

And we face serious questions of how supply chain vulnerability, which is reminding us about how security here in the U.S. is dependent upon the health of our Internet cybersecurity. Members on our side of the aisle even had a secure briefing on the potential threats and impacts to our own devices.
So it is important to remember that the Internet is a global network. No matter how secure we make our networks, we remain vulnerable to weaknesses abroad. This is why it is essential that we have a national strategy to deal with these threats.

We also need to work with our international partners to form coalitions around cybersecurity standards and work toward harmonizing privacy and cybersecurity regulations.

These latest privacy and security breaches and advancing cyber threats show that this problem is accelerating, but as you said, Mr. Chairman, there is also lots of opportunity for great applications, services, and devices that we all like. So it illustrates the complexity of the challenges we face.

Consumers are at the center of this and we cannot just require them to have a deeper understanding of the risks involved. We need to make sure that their devices and concerns are not just about notice and consent, but we have strong provisions here and a description that will help create a better culture. The best plain language notices, the clearest opt-in consent provisions, the most crystal clear transparency does not do any good when companies are being careless or willingly letting our data out the back door to third parties that have no relationship to the consumers. While the benefits of the online world are everywhere—and I truly mean that—everywhere—so must be the protection of personal information that is more than just a commodity. We need to make sure that the culture of monetizing our personal data at every twist and turn is countered with the protection of people’s personal data.

So Congress has to come to terms with this. I know that the members of this committee are working very diligently on trying to address that and that we are working to try to make sure that the things that happened in the 2016 election cycle also do not happen in the 2020 cycle. But these issues of information being stolen or manipulated or trying to influence or disrupt governments, even our own hacking of our employee personal information account, show that we are vulnerable and that we need to do more.

So the consistency of the hearings that we have had on this issue—I appreciate both Chairman Thune and you having these hearings about cybersecurity, about Equifax, about cyber hygiene, and what we should be doing—these all I believe should be part of the solution. Data security for Americans means that we extend the protections and we make sure that the online world is operating in a way that we see are helping to protect consumers and individual information.

So, Mr. Chairman, I know that you remain very dedicated to comprehensive legislation here. I do as well, even though the challenge is high. We need to have the opportunity to craft solutions that address security and privacy for the entire life cycle of our data and collection to storage and to processing. So hopefully today’s hearing will give us more input as to the way consumers look at this issue and what we can do to help us move forward. Thank you.

The Chairman. Thank you very much, Senator Cantwell.

And again, we welcome our witnesses. Your entire statements will be included in the record, and we ask each of you to summa-
rize your opening statements within five minutes. We will begin
down at this end of the table with Ms. Dixon. Welcome.

STATEMENT OF HELEN DIXON, COMMISSIONER, DATA
PROTECTION COMMISSION OF IRELAND

Ms. DIXON. Chairman Wicker, Ranking Member Cantwell, and
members of the Committee, thank you for inviting me to be here
today.
I am pleased to have the opportunity to share with the Com-
mittee the experience of the Irish Data Protection Commission in
dealing with complaints from consumers under EU data protection
law and hope it will be of assistance in your deliberations on a Fed-
eral privacy law.
As the Committee is aware, I submitted in advance a slightly
more expansive written statement to you than my five minutes
today will permit. So as suggested by the Chair, I will cover all of
its key points for you briefly now.
An important context in talking about EU data protection law is
the fact that the right to have one’s personal data protected exists
as an explicit fundamental right of EU persons under the EU
Charter of Fundamental Rights. It is the case then that the right
to data protection in the EU exists in all personal data processing
contexts and not just in commercial contexts.
The Committee is well aware I think at this stage of the basic
structure of the EU GDPR which sets out, firstly, obligations on or-
ganizations, then rights for individuals, and finally, provides for su-
 pervision and enforcement provisions to be implemented by inde-
pendent data protection authorities. As an EU regulation, it has di-
rect effect in every EU member state.
The obligations on organizations processing information that re-
lates to an identified or identifiable person are set down in a series
of high-level technology-neutral principles, so principles of lawfulness,
fairness, transparency, purpose limitation, data minimization,
accuracy, storage limitation, integrity, and confidentiality and ac-
countability.
The GDPR contains some prescription around new accountability
provisions and, in particular, requirements in certain cases to now
appoint a data protection officer. In addition there is an obligation
to notify breaches of personal data that give rise to risks for indi-
viduals to the data protection authority within 72 hours of the or-
ganization becoming aware of the breach.
In turn then, the individuals and consumers whose personal data
are processed have a series of enumerated rights under the GDPR.
These cover the right to transparent information, the right to ac-
cess to a copy of their personal data, the right to rectification, the
right to erasure, and so on. And each of these rights has varying
conditions pertaining to the circumstances in which those rights
can be exercised.
Finally, then the GDPR provides for independent and adequately
resourced data protection authorities in each EU member state. As
data protection authorities, we have a very broad range of tasks
that range from promoting awareness and issuing guidance on data
protection law, to encouraging industry codes of conduct, to han-
dling all valid complaints from consumers, and then investigating significant infringements of the GDPR.

The new one stop shop for multinationals under the GDPR means that the Irish Data Protection Commission is the lead supervisory authority in the EU for the vast majority of U.S. global Internet companies such as Facebook, Twitter, WhatsApp, Google, AirBnB, and Microsoft as these have their main establishment in Ireland.

The GDPR has introduced a much harder enforcement edge to EU data protection law with a range of corrective powers at the disposal of data protection authorities in addition to a capability to apply fines of up to 4 percent of the worldwide turnover of multinationals.

In the 11 months since GDPR came into application, the Irish Data Protection Commission has received in excess of 5,900 complaints from individuals. It is frequently a feature of the complaints we handle from consumers that their interest in their personal data is as a means of pursuing further litigation or action. So, for example, former employees of organizations often seek access to their personal data as part of the pursuit of an unfair dismissals case. Consumers may seek access to CCTV images in various different scenarios to pursue personal injuries cases and so on.

Overall, the most complained-against sectors in a commercial context are retail banks, telecommunications companies, and Internet platforms. And my written statement has provided you with some specific case studies and examples of the complaints we have handled.

Equally worth mentioning is the complainants to my office have rights to appeal and judicially review decisions of the Data Protection Commission, and my office is involved in over 20 litigation cases currently before the Irish courts. And the Committee might be interested to know that the vast majority of decisions appealed to court from my office relate to disputes between employers and employees and far fewer relate to commercial contexts.

Aside then from handling complaints, the Data Protection Commission has power to open investigations of its own volition, and we have 51 large-scale investigations underway covering the large tech platforms, amongst others.

So in conclusion, the EU data protection law places a very strong emphasis on the individual in light of the fundamental rights and strong emphasis on the exercise of the rights of the individual, and accordingly, it mandates the handling of every complaint from an individual by data protection authorities. This means the EU data protection authorities play an important dual role, on the one hand resolving high volumes of issues for individuals and on the other, supervising companies to ensure systemic issues of noncompliance are rectified and punished as appropriate.

The GDPR is 11 months old at this point, and clarity and consistency of standards will evolve in the coming years, driving up overall the standards of protection for consumers in every sector.

Thank you.

[The prepared statement of Ms. Dixon follows:]
PREPARED STATEMENT OF HELEN DIXON, COMMISSIONER,
DATA PROTECTION COMMISSION OF IRELAND

Introduction
Chairman Wicker, Ranking Member Cantwell and Members of the Committee,
thank you for inviting me to be here today.
I am pleased to have the opportunity to share with the Committee the experience
of the Irish Data Protection Commission in dealing with complaints from consumers
under the General Data Protection Regulation or GDPR, applicable since 25th May
2018. Clearly, in a global context, the GDPR represents one significant form of regu-
lation of the collection and processing of personal data and the Irish Data Protection
Commission’s approach to monitoring and enforcing its application provides an early
insight into the types of issues raised by consumers in complaints about how their
personal data is handled.

It’s useful for me to take a few minutes to set in context for you the circumstances
in which complaints from consumers are lodged with the Data Protection Commis-
sion.

The right to have one’s personal data protected exists as an explicit fundamental
right of EU persons under the EU Charter of Fundamental Rights that came into
legal force in 2009 and the right is called out specifically in Article 16 of the Treaty
on the Functioning of the European Union—the “Lisbon Treaty”. It is of course not
an absolute or unlimited right. It may be and often is subject to conditions or limita-
tions under EU and member state law but those conditions cannot render it impos-
ible for individuals to exercise core elements of the right to data protection. The
aim equally of a consistent and harmonised data protection law across the EU is
to ensure a level-playing field for all businesses and a consistent digital market in
which consumers can have trust. While many may argue that data privacy is now
“dead” given the ubiquitous nature of data collection in online environments, the
Data Protection Commission can nonetheless identify the clear benefits to con-
sumers of having exercisable and enforceable rights. (Dorraji, 2014)

The committee is well aware of the basic structure of the GDPR which sets out
a) obligations on organisations, b) rights for individuals, and c) enforcement provi-
sions. As an EU regulation, it has direct effect in every EU member state but also
has extra-territorial reach in that it applies to any overseas company targeting
goods or services at European consumers.

Obligations
Under the GDPR, a series of obligations apply to any organisation collecting and
processing information that relates to an identified or identifiable person. A broad
definition of personal data is in play with the GDPR specifying that identification
numbers, location data and online identifiers will be sufficient to bring data in
scope. The obligations on organisations are set down in a series of high-level, tech-
nology neutral principles: lawfulness, fairness, transparency, purpose limitation,
data minimisation, accuracy, storage limitation, integrity and confidentiality and ac-
countability.

Rights
In turn, the individuals whose personal data are processed have a series of enu-
erated rights under the GDPR. Incidentally, individuals under the GDPR are refer-
ced as “data subjects” which is a concept far broader than consumers given that
the GDPR concerns itself with any personal data processing and not merely that
which occurs in commercial contexts. However, I understand for the purposes of this
committee, that it is the subset of data subjects that are consumers and service
users that is of particular interest. The rights of consumers under the GDPR are
set out in Chapter 3 and cover the right to transparent information, the right of
access to a copy of their personal data, the right to rectification, the right to erasure,
the right to restriction of data processing, to object to certain processing and the
right to data portability with varying conditions pertaining to the circumstances in
which those rights can be exercised. And I will revert to these rights shortly when
I outline for the committee a profile of the complaints from consumers the Data Pro-
tection Commission is handling where consumers allege those rights are not being
delivered on by companies.

Enforcement Provisions
Finally, the GDPR provides for independent and adequately resourced data pro-
tection authorities in each EU Member State to monitor the application of the
GDPR and to enforce it (these authorities are separate and distinct from the con-
sumer protection and anti-trust authorities in the Member States). In this context,
data protection authorities have a very broad range of tasks from promoting aware-
ness, to encouraging industry codes of conduct to receiving notifications of the appointment of Data Protection Officers in companies to handling complaints from consumers and investigating potential infringements of the GDPR.

In general terms, the individual EU member state data protection authorities are obliged to handle every valid complaint from any individual in their member state and to supervise establishments in their territory. However, because of a new “one-stop-shop” innovation in the GDPR, multinational organisations operating across the EU can be supervised by one lead supervisory authority in the EU member state where that multinational has its “main-establishment”. Equally, any individual across the EU may lodge a complaint with the data protection authority in the member state of the main establishment of the company concerned. As a result, the Irish Data Protection Commission is the lead supervisory authority in the EU for the vast majority of U.S. global Internet companies such as Facebook, Twitter, WhatsApp, Google, AirBnB, Microsoft and Oath as they have their main establishments in Ireland. Equally, complaints are lodged with the Irish Commission from complainants across the EU either directly or via the supervisory authority in their own member state.

This may seem like a difficult computation given that there are potentially up to half a billion consumers in the EU. How can a data protection authority with currently 135 staff deal with complaints from across the EU and supervise so many large companies? Part of the answer lies in the orientation of the GDPR itself which places accountability to consumers directly on the shoulders of companies themselves. Companies must in many cases appoint Data Protection Officers; they must publish contact details for those officers and they must administer systems to allow them effectively handle requests from consumers to exercise their data protection rights. It’s therefore now the case that many issues arising for consumers are being resolved directly through the intervention of the mandatorily appointed Data Protection Officer in the company before there’s a need to file a complaint with the data protection authority. Many companies we supervise report to us that that have had a steep rise in consumer requests to exercise rights since the application of the GDPR in May 2018. Equally, EU data protection authorities can conduct joint operations where an authority like the Irish Commission can leverage specific expertise in another EU data protection authority in conducting an investigation. Further, multiple consumers may often raise the same issue as one another which may lead the Data Protection Commission to open an investigation of its “own volition” in order to resolve what may be a systemic matter. Finally, the threat of very significant administrative fines hangs over companies that fail to implement the principles of GDPR and/or deliver on consumer rights under the law with 4 percent of global turnover representing the outer but significant limit of fine that may be imposed.

Clearer Standards

Much of the success over the coming years of the GDPR will derive from the evolution of clearer, objective standards to which organisations must adhere. These standards will evolve in a number of ways:

- Through the embedding of new features of the GDPR such as Codes of Conduct, Certification and Seals that will drive up specific standards in certain sectors. Typically, codes of conduct that industry sectors prepare for the approval of EU data protection authorities will have an independent body appointed by the industry sector to monitor compliance with the code thereby driving up standards of protection and means by which consumers can exercise their rights.
- Through enforcement actions by the Data Protection Commission where the outcome, while specific to the facts of the case examined, will be of precedential value for other organisations. The Data Protection Commission currently has 50 large scale investigations running which, as they conclude in the coming months, will serve to set the mark for what is expected of organisations under the principles of transparency, fairness, security and accountability.
- Through case law in the national and EU courts, where data protection authority decisions are appealed or in circumstances where individuals use their right of action under the GDPR to claim compensation for any material or non-material damage they have suffered arising from an infringement of the GDPR.
- Through the provision of further guidance to organisations on specific data processing scenarios particularly through published case studies of individual complaints the Data Protection Commission has handled. Equally, guidance will be published off the back of consultations with all stakeholders on how to implement principles in complex scenarios such as those involving children where specific protections and consideration of the evolving capacities of the child need to be factored in.
Consumer Complaints

In the 11 months since GDPR came into application, the Data Protection Commission has received 5839 complaints from individuals. It is frequently a feature of complaints we handle from consumers that their interest in their personal data is as a means of pursuing further litigation or action. For example, former employees of organisations often seek access to their personal data as part of the pursuit of an unfair dismissals case; consumers seek access to CCTV images in different scenarios to pursue personal injuries cases and so on.

Overall, the most complained against sectors in a commercial context are retail banks, telecommunications companies and Internet platforms.

In the cases of the retail banks and telecommunications providers, the main issues arising relate to consumer accounts, over-charging, failure to keep personal data accurate and up-to-date resulting in mis-directing of bank or account statements, processing of financial information for the purposes of charging after the consumer has exercised their right to opt-out during the cooling-off period. While you might argue that these are clearly predominantly customer service and general consumer issues, it is the processing of their personal data and in particular deductions from their bank accounts that bring consumers to the door of the Data Protection Commission.

In terms of the Internet platforms, individuals, as well as Not-for-profit organisations on their behalf that specialise in data protection, raise complaints about the validity of consent collected for processing on sign-up to an app or service, the transparency and adequacy of the information provided and frequently about non-responses from the platforms when they seek to exercise their rights or raise a concern. Further, the Data Protection Commission has received several complaints about the inability of individuals to procure a full copy of their personal data when they request it from a platform. This can arise in scenarios where platforms have instituted automated tools to allow users by self-service to download their personal data but elements of data are not available through the tool. In one such complaint we are handling, the user complains that significant personal data is held in a data warehouse by a platform and used to enrich the user’s profile. The platform argues that access to the data is not possible because it’s stored by date and not individual identifier and further that the data would be unintelligible to a consumer because of the way it’s stored. The Data Protection Commission must resolve whether this is personal data to which a right of access applies.

Other cases dealt with this year by the office relate to financial lenders required to notify details to the Irish Central Bank of credit given to individual consumers. Certain lenders notified the details twice resulting in adverse credit ratings for the individuals as they appeared to have 2 or 3 times the number of loans as compared to what they actually had. In another case, a multinational agent dealing by web chat with a service user about a customer service complaint took note, according to the complaint received by the office, of the consumer’s personal details including mobile ‘phone number she used to verify her account and contacted the user asking her on a date. That didn’t turn out to be a happily-ever-after story when independently of the investigation of my office, the agent was removed from his job!

A further complaint dealt with was lodged by an individual who had suffered a family bereavement. A tombstone company issued immediate correspondence to her family advertising cheap headstones in respect of the dead relative. The tombstone company had taken data from an online death notice website and recreated the full address from multiple other sources. The actions of the company were not only distasteful but in breach of the purpose limitation requirements of data protection law.

A particularly concerning case was reported to the office six months ago concerning a mobile ‘phone user whose ex-partner had managed to verify identity with her mobile telephone provider by masquerading as the individual herself and gained control of her telephone number. He did this by contacting the telco via web chat and when asked to identify himself, he provided her name and mobile ‘phone number. He then told the customer service agent at the telco that he (masquerading as her) had lost his mobile ‘phone, had now purchased a new SIM card and requested that the ‘phone number be ported over to the new SIM he had bought. The agent asked the imposter the following verification questions:

- What is your full address? Answered correctly
- What are 3 frequently dialled numbers? Could not answer
- Can you tell me your last top-up date? Could not answer
- Can you tell me your last top-up amount? Answered correctly

Despite the imposter not answering all of the questions, the agent accepted this as valid authentication, and ported the complainant’s number onto the imposter’s
newly bought SIM card. This gave access to any future texts and calls coming to the complainant's phone number. This would allow for example the imposter to bypass the phone number factor for authentication with her online banking account. In this case, the telco had failed to adhere to its own standards for verification of identity with very unfortunate consequences.

Parallel but overlapping laws to the GDPR specific to E-Privacy are equally enforced by the Data Protection Commission and annually the office prosecutes a range of companies for multiple offences. In the majority of cases, these relate to targeting of mobile phone users with marketing SMS messages without their consent and/or without providing the user with an OPT OUT from the marketing messages. Equally, a number of companies are prosecuted annually where they offer an OPT OUT but fail to apply it on their database resulting in the user continuing to receive SMS messages without their consent. As a result of several years of consistent high-profile prosecutions in this area, the Data Protection Commission considers the rate of compliance appears to be improving.

Considerable resources of the office have been applied in recent years to a series of investigations into the “Private Investigator” sector. The Data Protection Commission received complaints from individuals who had lodged claims with their insurance providers and later became concerned about how their insurance company had sourced particular information about them and used it to deny their claims. The Data Protection Commission uncovered a broad-ranging national “scam” involving a considerable number of private investigator or tracing companies that had been either bribing or blagging government officials and utility company staff in some cases to procure a range of pieces of personal information about the claimants. 5 companies and 4 company directors were successfully prosecuted by the Data Protection Commission for these data protection offences over the last 4 to 5 years.

The final case I’ll mention in a commercial context is the case of an individual who suffered an accident giving rise to a leg injury. When her claim to her insurance company was denied, she sought access to a copy of her personal data that had been used by the company to deny her claim as she was surprised at the reasons given. She discovered on receipt of her personal data, that her family doctor had, instead of sending a report detailing information about the nature of her leg injury suffered in the recent accident, sent the entire file of 30 plus years of consultations between him and the patient to the insurance company. The company used very sensitive information about another condition the woman had suffered from years previously to deny the claim. Aside from the denial of the claim, the complainant suffered considerable distress at the thought of a very sensitive and irrelevant set of information about her having been disclosed and then processed in this matter.

This office found the family doctor had infringed data protection law in disclosing excessive personal data including sensitive personal data. Ultimately, this complainant pursued a civil claim for compensation in the courts and the case settled on the steps of the court.

Outside of these commercial contexts, a large volume of complaints that come to the Commission relate to access requests where an individual considers they have been denied access to a copy of the personal data they requested from an organisation. In the majority of cases, the Data Protection Commission amicably resolves these cases which in an access request scenario means we ensure the individual receives all of the personal data to which they’re entitled. This may of course be less than they sought as an organisation may legitimately apply exemptions where it is lawful to do so.

The Committee will be well aware of various academic studies on the so-called “privacy paradox” where discrepancies between our attitudes as online users and our behaviours are apparent. This is a complex area of study but I raise it by way of pointing out that consumer complaints alone may not give us a very complete picture of what concerns consumers or what elements of the controls provided by platforms are useful to them. The platforms don’t publish data on user engagement with their privacy control dashboards and the frequency with which users complete “privacy checkup” routines prompted by the platforms but based on data they have shared with the Data Protection Commission, the number of users seeking to engage with and control their settings is significant. Of course, this leads us then to the issues raised by Dr Zeyneb Tufekci in the recent New York Times privacy series on whether being “discreet” online protects users and where she concludes that powerful computational inferences make it unlikely discretion is of much assistance.
Large-scale Investigations

This brings me then to the important work of the Data Protection Commission outside of the role in handling complaints from individuals. In many ways, effective implementation of principles of fairness, transparency, data minimisation and privacy by design will negate the need for users and consumers to have the responsibility for ensuring their own protection thrust entirely upon them through making decisions about whether to "consent" or not.

The Data Protection Commission has powers to open an investigation of its own volition or may opt to open an investigation into a complaint from an individual that discloses what appears to be a systemic issue that potentially affects hundreds of millions of users.

The Data Protection Commission has currently 51 large-scale investigations underway. 17 relate to the large tech platforms and span the services of Apple, Facebook, LinkedIn, Twitter, WhatsApp and Instagram. Because the GDPR is principles-based and doesn’t explicitly prohibit any commercial forms of personal data processing, each case must be proved by tracing the application of the principles in the GDPR to the processing scenario at issue and demonstrating the basis upon which the Commission alleges there is a gap between the standard we say the GDPR anticipates and that which the company has implemented. The first sets of investigations will conclude over the summer of 2019.

Redress

EU data protection authorities resolve complaints of individuals amicably for the most part and where amicable resolution is not possible, the action of the authority is directed against the processing organisation. Authorities do not order redress in the form of payment of damages to individuals whose rights have been infringed.

In order to secure damages, individuals have a right of action under Article 82 GDPR where they or a not-for-profit representing them can bring a case through the courts to seek compensation for material or non-material damage they allege they have suffered as a result of infringements of the GDPR. Such Article 82 actions for compensation by individuals in the Irish courts have not yet been heard but when these are, they will represent further clarifications on how the courts view the GDPR and its application.

No class action system exists in Ireland and in general this is not a feature of the EU landscape. While there are some reports emanating particularly from the UK that representative actions are being lined up by some law firms on a “no win no fee” basis post large-scale breaches being notified, nothing of significance has materialised in this regard. (Osborne Clarke—GDPR one year on: how are EU regulators flexing their muscles and what should you be thinking about now?)

Conclusion

EU data protection law places a strong emphasis on the individual and the exercise of their rights and accordingly mandates the handling of every complaint from an individual by data protection authorities. This means EU data protection authorities play an important dual role—on the one hand, resolving high volumes of issues for individuals and on the other supervising companies to ensure systemic issues of non-compliance are rectified and punished as appropriate. The GDPR is 11 months old and clarity and consistency of standards will evolve in the coming years driving up standards of data protection for consumers in every sector.

References


(n.d.). Osborne Clarke—GDPR one year on: how are EU regulators flexing their muscles and what should you be thinking about now? 2019 Lexology: daily subscriber feed.


The CHAIRMAN. Thank you very much, Ms. Dixon.

Mr. Polonetsky.
STATEMENT OF JULES POLONETSKY, CHIEF EXECUTIVE OFFICER, FUTURE OF PRIVACY FORUM

Mr. POLONETSKY. Thank you, Chairman Wicker, Ranking Member Cantwell, Committee members.

Eighteen years ago, I left my job as the New York Consumer Affairs Commissioner to become one of the first wave of Chief Privacy Officers when that was yet a novel title. Today as CEO of FPF, I work with the CPOs of more than 150 companies, with academics, with civil society, and with leading foundations on the privacy challenges posed by tech innovations.

I first testified before this Committee almost 20 years ago to address privacy concerns around behavioral advertising. And almost every day since, we have seen those reports of new intrusions, new risks, new boundaries crossed. Sometimes it is simply a company being creepy. Sometimes it is a practice that raises serious risks to civil liberties or our sense of autonomy.

It is long past time to put a privacy law in place that can support that trust that Americans should have when they use their phones, when they surf the Internet, when they shop online, all of the activities of daily life. Every day we delay, it becomes harder. New businesses launch. New technologies are developed and become entrenched.

At the same time, we are, of course, benefiting from many of these technologies, as you both mentioned, companies reinventing mobility and making transportation safer. Machine learning has been built into so many of the products and services, health care diagnosis, education tech providers working on personalized learning. Every one of these holds great promise. Every one of them also brings new perils.

It is a global challenge, of course, and almost every leading economy, not just our European colleagues, have put comprehensive laws in place. Japan. We should take special note perhaps of the APEC CBPRs, the Asia-Pacific region where the U.S. has played a long role and which we have recently committed to in the proposed treaty for trade between U.S., Mexico, and Canada. We should not be left behind as the standards that are actually defining technologies today and the terms of trade for a decade to come are being established. Even small businesses do business globally today via the Web and need that guidance.

So a baseline law should have strong protections matching and exceeding the key rights of California’s privacy law: transparency, access, deletion, the right to object, protections for minors, the right to object to sales of data. But we also need to add some of the other core privacy principles that are not included in CCPA. Compatible use, contexts, special restrictions on sensitive data, the full range of fair information practices, as they have been reflected in so many of the national and international models, and many which originated back in the 1970s in the U.S. should be in our law.

In drafting, we should be clear about what is covered. If we do not know what is personal, we do not know what is in and what is out. But I would argue that this is not a binary in or out decision. Information is not either completely explicitly personal and it is probably never completely anonymous. There are stages of data, and a law that is careful would nuance different levels of rights
and restrictions based on whether data is fully anonymous, whether it is pseudonymous. The actual different stages in the lifestyle are the best way to match the corresponding requirements.

Research has not always been handled well in a number of the legislative models around the world. We want to, I think, encourage beneficial research if it is being carried out in a way that supports privacy, fairness, equity, the integrity of the scientific process. We should encourage legitimate research when the appropriate ethical reviews are in place.

And at the end of the day, internal accountability mechanisms are how organizations actually make sure they follow the law. We do not want just privacy in the law. We want it on the ground. We want privacy by design, and that means employees that are trained. That means tools and systems that support responsible data stewardship. So laws should encourage comprehensive programs, and whenever possible, we should incentivize PETs, privacy enhancing technologies, that deliver us perhaps the benefits of data while making sure that we have strong mathematical proofs that we have minimized any risks.

And of course, any law is going to impact the sectoral State privacy laws that have been passed in recent decades. We certainly should avoid a framework where a website operator or a small business should have to deal with a complexity of inconsistent State mandates on many of the day-to-day issues of operating a business. But these concerns can be reasonably avoided with carefully crafted Federal preemption. There are clearly core State privacy laws that can and must exist, student privacy laws and others, and that I think is an important challenge for the Committee.

But laws are only as good as enforcement. The FTC should have not only the civil penalties, not only the careful targeted rule-making, but it also should have education and outreach so that new businesses understand, can get their questions answered. The FTC needs both the carrot and the stick.

And of course, State AGs, who have been such critical partners to our Federal leaders, should continue to have a role.

Thank you for the chance to share those thoughts with you today.

[The prepared statement of Mr. Polonetsky follows:]

PREPARED STATEMENT OF JULES POLONETSKY, CHIEF EXECUTIVE OFFICER, FUTURE OF PRIVACY FORUM

Thank you for inviting me to speak today. The Future of Privacy Forum is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. We are supported by leading foundations, as well as by more than 150 companies, with an advisory board representing academics, industry, and civil society. We bring together privacy officers, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

I speak to you today with a sense of urgency. Congress should advance a baseline, comprehensive Federal privacy law because the impact of data-intensive technologies on individuals and vulnerable communities is increasing every day as the pace of innovation accelerates. Each day’s news brings reports of a new intrusion,
new risk, new harm, another boundary crossed. Sometimes it’s a company doing something that consumers or critics regard as “creepy;” sometimes it is a practice that raises serious risks to our human rights, or civil liberties, or our sense of autonomy. There is a growing public awareness of how data-driven systems can reflect or reinforce discrimination and bias, even inadvertently.2

For many people, personal privacy is a deeply emotional issue, and a real or perceived absence of privacy may leave them feeling vulnerable, exposed, or deprived of control. For others, concrete financial or other harm may occur; a loss of autonomy, a stifling of creativity due to feeling surveilled, or the public disclosure of highly sensitive information like individuals’ financial data or disability status are just some potential consequences of technology misuse, poor data security policies, or insufficient privacy controls.3

At the same time, individuals and society are benefitting from new technologies and novel uses of data. Companies reinventing mobility are making transportation safer and more accessible; healthcare providers are using real-world evidence to advance research; and education technology providers can empower students and teachers to enhance and personalize learning.4 In much the same way that electricity faded from novelty to background during the industrialization of modern life 100 years ago, we see artificial intelligence and machine learning becoming the foundation of commonly available products and services, like voice-activated digital assistants, traffic routing, and accurate healthcare diagnoses.5

Each of these examples holds the promise of improving our lives but each one also poses the risk of new and sometimes unforeseen harms. It is in the best interests of individuals and organizations for national lawmakers speak in a united, bipartisan voice to create uniform protections that help rebuild trust. Congress has the opportunity now to pass a law that will shape these developments to maximize the benefits of data for society while mitigating risks. Delaying Congressional action means that businesses will inevitably continue to develop new models, build infrastructure, and deploy technologies, without the guidance and clear limits that only Congress can set forth.

This is a global challenge, and other countries have responded. The European Union (EU) has substantially updated its data protection framework, the General Data Protection Regulation (GDPR),6 and Japan has made substantial updates to its data protection law, the Act on Protection of Personal Information (APPI).7 The EU and Japan have also announced a trade agreement that includes a reciprocal data adequacy determination, creating the world’s largest exchange of safe data flows and boosting digital trade between the two zones.8 Other nations, from India9 to Brazil,10 are passing privacy laws or updating existing data protection regimes.11 Current business practices along with new technologies are being shaped by laws around the world, while the U.S. approach to data protection remains outdated and insufficient. The continuation of cross-border data flows, which are crucial to the United States’ leadership role in the global digital economy, are under stress. This may put U.S. companies, from financial institutions to cloud providers, at a disadvantage due to the perception that our laws are inadequate. Congress must en-

---

10 Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais (Brazil General Data Protection Law).
sure that the U.S. is not left behind as the rest of the world establishes trade and privacy frameworks that will de facto define the terms of international information and technology transfers for decades to come.

The United States currently does not have a baseline set of legal protections that apply to all commercial data about individuals regardless of the particular industry, technology, or user base. For the past decades, we have taken a sectoral approach to privacy that has led to the creation of Federal laws that provide strong protections only in certain sectors such as surveillance, healthcare, video rentals, education records, and children’s privacy. As a result, U.S. Federal laws currently provide strong privacy and security protection for information that is often particularly sensitive about individuals but it leaves other data largely unregulated aside from the FTC’s Section 5 authority to enforce against deceptive or unfair business practices. For example, health records held by hospitals and covered by the Health Insurance Portability and Accountability Act (HIPAA) are subject to strong privacy and security rules, but health-related or fitness data held by app developers or online advertising companies is not covered by HIPAA and is largely unregulated. Student data held by schools and covered by the Family Educational Rights and Privacy Act (FERPA) is subject to Federal privacy safeguards, but similar data held by educational apps unaffiliated with schools is not subject to special protections. The Fair Credit Reporting Act (FCRA) helps ensure the accuracy of third-party information used to grant or deny loans, but FCRA’s accuracy requirements do not apply to similar third-party reviews used to generate user reputation scores on online services.

The U.S. has not always lagged behind its major trade partners in privacy and data protection policymaking. In fact, the central universal tenets of data protection have U.S. roots. In 1972, the Department of Health, Education, and Welfare formed an Advisory Committee on Automated Data Systems, which released a report setting forth a code of Fair Information Practices. These principles, widely known as the Fair Information Practice Principles (FIPPs), are the foundation of not only existing U.S. laws but also many international frameworks and laws, including GDPR. And while GDPR is the most recent major international legislative effort, the U.S. should look for interoperability with and insights from the OECD Privacy Guidelines and the Asia-Pacific Economic Cooperation (APEC) framework and Cross-Border Privacy Rules (CBPRs).

As privacy concerns continue to escalate, states around the U.S. are charging ahead, proposing, passing, or updating consumer privacy laws. Many of these laws...
are serious, nuanced efforts to provide individuals with meaningful privacy rights and give companies clarity regarding their compliance obligations. At the same time, multiple, inconsistent state law requirements risk creating a conflicting patchwork of laws that create uncertainty for organizations that handle personal information. Individuals deserve consistent privacy protections regardless of the state they happen to reside in.

The U.S. has a shrinking window of opportunity to regain momentum at both the national and international level. If we wait too long, more countries will act, which will have an immediate impact on new technologies and business initiatives and ultimately reduce the impact of any Federal law.

There are key points that need to be addressed with particular care in any Federal consumer privacy law. A baseline Federal privacy law should offer strong protections. This, in turn, will bolster trust in privacy and security practices. The law will regulate a substantial share of the U.S. economy, and must therefore be drafted with careful attention to its effects on every sector as well as a wide range of communities, stakeholders, and individuals.

Eighteen years ago, I left my job as the New York City Consumer Affairs Commissioner to become one of the first company chief privacy officers (CPO) in the U.S. Working for eight years in privacy and consumer protection roles at major tech companies helped me understand that it takes people, systems, and tools to manage data protection compliance. I have also served as a state legislator and a Congressional staffer, and today at FPF work with companies, foundations, academics, regulators, and civil society to seek practical solutions to privacy problems. With this perspective, gained from my experience with key stakeholder groups and ongoing focus on the protection of privacy of individuals and consumers, I offer the following views.

1. Covered Data and Personal Information Under a Federal Privacy Law

In drafting baseline Federal privacy legislation, the most important decision is one of scope: how should the law define the "personal information" that is to be protected? Laws that adopt an overly broad standard are forced to include numerous exceptions in order to accommodate necessary or routine business activities, such as fraud detection, security, or compliance with legal obligations; or to anticipate future uses of data, such as scientific research or machine learning. Conversely, laws that define personal information too narrowly risk creating gaps that allow risky uses of data to go unregulated.

Leading government and industry guidelines recognize that data has a range of linkability where it can potentially be used to identify or contact an individual or to customize content to an individual person or device. According to the Federal Trade Commission (FTC), data are not “reasonably linkable” to individual identity to the extent that a company: (1) takes reasonable measures to ensure that the data are deidentified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the “Three-Part Test”). Federal Trade Commission, Protection Consumer Privacy In An Era of Rapid Change (2012), at 21, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumerprivacy-era-rapid-change-recommendations/120326privacyreport.pdf. According to the National Institute of Sciences and Technology (NIST), “all data exist on an identifiability spectrum. At one end (the left) are data that are not related to individuals (for example, historical weather records) and therefore pose no privacy risk. At the other end (the right) are data that are linked directly to specific individuals. Between these two endpoints are data that can be linked with effort, that can only be linked to groups of people, and that are based on individuals but cannot be linked back.” Simon L. Garfinkel, NISTIR 8053, De-Identification of Personal Information (Oct. 2015), at 5, http://nvlpubs.nist.gov/nistpubs/lapr/2015/NIST.IR.8053.pdf. Leading industry associations provide similar guidelines. See e.g., Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data (Nov 2011), at 8, available at http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf

26 Leading scholars and advocates have expressed skepticism about market-based responses to privacy and security concerns. Common criticisms of a purely market-driven approach include: consumers’ lack of sophistication with respect to data security (See, e.g., Aaron Smith, What the Public Knows About Cybersecurity, Pew Research Center (Mar. 22, 2017), http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/ last accessed on Nov. 9, 2018); the typical length and substance of modern privacy notices (See e.g., Alecia M. McDonald and Lorrie Faith Cranor, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society, at 8–10, (2008)); research suggesting that most individuals do not adequately value future risks (See e.g., Chris Jay Hoofnagle & Jennifer M. Urban, Alan Westin’s Privacy Homo Economicus, 49 Wake Forest L. Rev. 261, 303–05 (2014)); the design of user interfaces to encourage decisions that are not aligned with users’ best interests (See Woodrow Hartzog, Privacy’s Blueprint: The Battle to Control the Design of New Technologies (2015)); and a lack of sufficient protections for privacy as an economic externality or “public good” (Joshua A. T. Fairfield and Christoph Engel, Privacy As A Public Good, 65 Duke L.J. 385, 423–25 (2015)).
should avoid classifying covered data in a binary manner as either “personal” or “anonymous.” Instead, it should draw distinctions between different states of data given their materially different privacy risks. Context matters. Personal data that is intended to be made public should be regulated differently than personal data that will be kept confidential by an organization. Similarly, data that is out in the wild should not be treated the same as data that is subject to technical deidentification controls (such as redacting identifiers, adding random noise, or aggregating records) as well as to effective legal and administrative safeguards (such as commitments not to attempt to re-identify individuals or institutional access limitations).

FPF has crafted modular draft statutory language that attempts to capture these distinctions. We believe, in broad terms, that categories of data that are exposed to individual privacy and security risks, yet materially different in their potential uses and impact, include:

- **Identified data:** information explicitly linked to a known individual.
- **Identifiable data:** information that is not explicitly linked to a known individual but can practically be linked by the data holder or others who may lawfully access the information.
- **Pseudonymous data:** information that cannot be linked to a known individual without additional information kept separately.
- **deidentified data:** (i) data from which direct and indirect identifiers have been permanently removed; (ii) data that has been perturbed to the degree that the risk of re-identification is small, given the context of the data set; or (iii) data that an expert has confirmed poses a very small risk that information can be used by an anticipated recipient to identify an individual.

By recognizing such distinctions, Federal privacy legislation would craft tiers of safeguards that are commensurate to privacy risks while at the same time allowing for greater flexibility where it is warranted. For example, on the one hand, appropriate regulatory requirements for deidentified data might mandate that companies cannot make such data public or share it with third parties without technical, administrative, and/or legal controls that reasonably prevent re-identification. But it may be appropriate to exempt deidentified data from other requirements, such as providing users with access or portability rights or the right to object to or opt-out of a company’s use of deidentified data, since by definition it is not technically feasible to link deidentified data to a particular, verifiable individual. On the other hand, for pseudonymous or identifiable data that can be reasonably linked to a known individual, it may be more fitting to provide individuals with access and portability rights, or the ability to opt-in or opt-out of certain uses of that data, as appropriate.

In many cases, the ability to reduce the identifiability of personal data through technical, legal, and administrative measures will allow a company to retain some utility of data (e.g., for research, as we discuss below), while significantly reducing privacy risks. New advances in deidentification and related privacy-enhancing technologies (PETs) (discussed below at number 5) are continuing to emerge. As a result, it is wise for lawmakers to take account of the many states of data and to pro-

---


29 See Appendix D.


31 Direct identifiers are data that directly identifies a single individual, for example names, social security numbers, and e-mail addresses. Indirect identifiers are data that by themselves do not identify a specific individual but that can be aggregated and “linked” with other information to identify data subjects, for example birth dates, ZIP codes, and demographic information. Simson L. Garfinkel, NISTIR 8055, De-Identification of Personal Information (Oct. 2015), at 15, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8055.pdf.

32 See section 3 below.

33 See section 5 below.
vide incentives for companies to use technical measures and effective controls reduce the identifiability of personal data wherever appropriate.

2. Sensitive Data

The term sensitive data is used to refer to certain categories of personal data that require additional protections due to the greater risks for harm posed by processing or disclosing this data. While individuals should generally be able to exercise reasonable control over their personal information, those controls should be stronger with respect to sensitive data. Thus, a Federal privacy law should provide heightened protections for the collection, use, storage, and disclosure of users’ sensitive personal information or personal information used in sensitive contexts. FPF has crafted modular draft statutory language that proposes a practical approach to regulating sensitive data that is consistent with current norms and best practices.\(^{34}\) The Federal Trade Commission has defined sensitive data to include, at a minimum, data related to children, financial and health information, Social Security numbers, and precise geolocation data.\(^{35}\) The GDPR defines sensitive data more broadly by recognizing special categories of personal data as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.”\(^{36}\) Under GDPR, the legal grounds for processing these special categories of data are more restricted.\(^{37}\)

In addition to opt-in controls, Federal legislation should include additional requirements—such as purpose limitation and respect for context—for certain sensitive categories of data. For example, if information such as a user’s precise geolocation or health information is collected with affirmative consent for one purpose (such as providing a location-based ridesharing service, or a fitness tracking app), a law should restrict sharing that sensitive, identifiable information with third parties for materially different purposes without user consent. This is consistent with the choice principle in the FTC’s 2012 Report, which urged companies to offer the choice at the point in time, and in a context, in which a consumer is making a decision about his or her data.\(^{38}\) There may be instances where sensitive data will require consent, and where such consent will be impossible to obtain.\(^{39}\) The law should provide for the creation of a transparent, independent ethical review process that can assess such cases and provide a basis for a decision that a use of data is beneficial and will not result in harm.

3. Research

It is vital that a national privacy law be crafted in a way that does not unduly restrict socially beneficial research, and that policymakers at the local, state, and Federal levels continue to have the information they need to make evidence-based decisions. Today, in addition to the entities governed by the HIPAA Rule and legal mandates around human subject research, many private companies also conduct research, or work in partnerships with academic researchers, to gain important insights from the data they hold.

While obtaining individuals’ informed consent may be feasible in controlled research settings, it is often impossible or impractical for researchers studying databases that contain the footprints of millions, or indeed billions, of data subjects. For example, when researchers are studying the effectiveness of personalized learning tools or evaluating disparate impacts of automated systems, they can benefit from access to large datasets. Legal mandates that require data holders to obtain continual permission from individuals for future uses of data—while appropriate in many commercial contexts—may create undue burdens for researchers who rely on

\(^{34}\) See Appendix D.


\(^{36}\) GDPR, Art 9.

\(^{37}\) GDPR, Art 9, Recital 51–52.


\(^{39}\) For example, recruiting individuals for rare disease drug trials.

datasets that contain information about individuals who cannot be contacted or who have been deidentified, particularly if researchers do not know, at the point of collection, what insights future studies may reveal. This does not mean that data-based research should be exempted from a Federal privacy law. The use of private commercial data for socially beneficial research should remain subject to strict standards for privacy, security, scientific validity, and ethical integrity. However, we recommend that legal frameworks contain flexible provisions for research, such as enforceable voluntary compliance with Federal Common Rule for human subject research; carefully tailored exceptions to the right of deletion for less readily identifiable information; or the creation of independent ethical review boards to oversee and approve beneficial research using personal information.

This balance between facilitating data research and evidence-based decision-making while maintaining privacy and ethical safeguards aligns with the 2017 report of the bipartisan Commission on Evidence-Based Policymaking and the 2018 Foundations for Evidence-Based Policymaking Act. The Commission noted that increasing access to confidential data need not necessarily increase privacy risk. Rather, “steps that can be taken to improve data security and privacy protections beyond what exists today, while increasing the production of evidence.”

In short, companies that conduct research or partner with academic institutions must do so in a way that protects privacy, fairness, equity, and the integrity of the scientific process, and a Federal privacy law should encourage, rather than place undue burdens on, legitimate research when appropriate ethical reviews take place.

4. Internal Accountability and Oversight

A Federal baseline privacy law should incentivize companies to employ meaningful internal accountability mechanisms, including privacy and security programs, which are managed by a privacy workforce. Ultimately, to implement privacy principles on the ground, including not just legal compliance but also privacy by design and privacy engineering, organizations will need to devote qualified and adequately trained employees. Indeed, over the past two decades, a privacy workforce has developed that combines the fields of law, public policy, technology, and business management. This workforce’s professional association, the International Association of Privacy Professionals (IAPP), has doubled its membership in just the past 18 months. The IAPP provides training and professional certification, demonstrating the heightened demand among organizations for professionals who manage data privacy risks.

In their book Privacy on the Ground, Kenneth Bamberger and Deirdre Mulligan stress “the importance of the professionalization of privacy officers as a force for transmission of consumer expectation notions of privacy from diverse external stakeholders, and related ‘best practices,’ between firms.” Accordingly, today, data privacy management should no longer be regarded as a role that employees in legal or HR departments fulfill as a small piece of their larger job. Rather, it must be a new professional role with standards, best practices, and norms, which are widely agreed upon not only nationally but also across geographical borders. Responsible practices for personal data management are not common knowledge or intuitive, any more than accounting rules. They require training, continuous education, and verifiable methods for identifying and recognizing acceptable norms. Put simply, the digital economy needs privacy professionals. Encouraging organizations to implement internal governance programs that employ such professionals will ensure higher professional standards and more responsible data use, regardless of the specific rules ultimately chosen for data collection, processing, or use.

41In the words of danah boyd and Kate Crawford, “It may be unreasonable to ask researchers to obtain consent from every person who posts a tweet, but it is problematic for researchers to justify their actions as ethical simply because the data are accessible. Future of Privacy Forum, Conference Proceedings: Beyond IRBs: Designing Ethical Review Processes for Big Data Research (Dec. 20, 2016), page 4, https://fpf.org/wp-content/uploads/2017/01/Beyond-IRBs-Conference-Proceedings_12-20-16.pdf, citing danah boyd & Kate Crawford, Critical Questions for Big Data, 15(5) INFO. COMM. & SOC. 662 (2012).

42The Commission noted that increasing access to confidential data need not necessarily increase privacy risk. Rather, “steps that can be taken to improve data security and privacy protections beyond what exists today, while increasing the production of evidence.”

Federal legislation could provide a safe harbor or other incentives for development, documentation, and implementation of comprehensive data privacy programs; execution of ongoing, documented privacy and security risk assessments, including for risks arising from automated decision-making; and implementation of robust accountability programs with internal staffing and oversight by senior management. For example, GDPR requires companies to document their compliance measures,\(^\text{46}\) appoint Data Protection Officers,\(^\text{47}\) and create data protection impact assessments,\(^\text{48}\) among other requirements. Another way to increase internal expertise is to incentivize employee training through recognized programs.

External certification processes act as objective validators to help companies, particularly those with limited resources, navigate complex legal requirements. Similarly, incentivizing companies or industry sectors to create "red teams" to proactively identify privacy abuses or to cooperate with watchdog entities or independent monitors to support additional oversight, such as through safe harbors or other methods, would create an additional layer of privacy safeguards.

5. Incentives for Technical Solutions

Federal privacy legislation should promote the use of technical solutions, including privacy-enhancing technologies (PETS). The "holy grail" for data protection is utilizing technology that can achieve strong and provable privacy guarantees while still supporting beneficial uses. Legislation should create specific incentives for the use of existing privacy-enhancing technologies and for the development of new PETS. Following are ten PETS or technological trends that may become increasingly useful tools to manage privacy risks:

Advances in Cryptography

\textbf{a. Zero Knowledge Proofs}—Zero knowledge proof (ZKPs) are cryptographic methods by which one party can prove to another party that they know something to be true without conveying any additional information (like how or why the mathematical statement is true). ZKPs can be used in identity verification contexts, e.g., to prove that someone is over a certain age without revealing their exact date of birth. ZKPs help with data minimization and data protection and promote privacy by design and default.

\textbf{b. Homomorphic Encryption}—Homomorphic encryption is a process that enables privacy-preserving data analysis by allowing some types of analytical functions and computations to be performed on encrypted data without first needing to decrypt the data.\(^\text{49}\) It is especially useful in applications that retain encrypted data in cloud storage for central access.

\textbf{c. Secure Multi-Party Computation}—Secure multi-party computation (SMPC) is a distributed computing system or technique that provides the ability to compute values of interest from multiple encrypted data sources without any party having to reveal their private data to the others. A common example is secret sharing, whereby data from each party is divided and distributed as random, encrypted "shares" among the parties, and when ultimately combined can provide the desired statistical result.\(^\text{50}\) If any one share is compromised, the remaining data is still safe. SMPC holds particular promise for sharing or managing access to sensitive data such as health records.

\textbf{d. Differential Privacy}—Differential privacy (DP) is a rigorous mathematical definition of privacy that quantifies the risk that an individual is included in a data set. It leverages anonymization techniques that involves the addition of statistical "noise" to data sets before calculations are computed and results released. DP can be global or local.\(^\text{51}\) Global DP is server-side anonymization or deidentification (where trust resides in the service provider); local DP is applied on the client or user's device. There are now differentially private versions of algorithms in machine learning, game theory and economic mechanism design, statistical estimation, and streaming. Differential privacy works

\(^{46}\)GDPR, Art. 24, 40.
\(^{47}\)GDPR, Art. 37–39.
\(^{48}\)GDPR, Art. 35.
\(^{49}\)See David Wu, University of Virginia Computer Science Department, available at [https://www.cs.virginia.edu/dwu4/fhe-project.html].
\(^{50}\)See Christopher Sadler, Protecting Privacy with Secure Multi-Party Computation, New America (Jan. 11, 2018), [https://www.newamerica.org/oti/blog/protecting-privacy-secure-multi-party-computation/].
\(^{51}\)Evaluation of Privacy-Preserving Technologies for Machine Learning, Outlier Ventures Research (Nov. 2018), [https://outlierventures.io/research/evaluation-of-privacy-preserving-technologies-for-machine-learning/].
better on larger databases because as the number of individuals in a database grows, the effect of any single individual on a given aggregate statistic diminishes.

Localization of Processing

e. Edge computing and Local Processing—For devices where speed is of the essence or connectivity is not constant, applications, data, and services are increasingly run away from centralized nodes at the end points of a network. Such local processing helps with data minimization by reducing the amount of data that must be collected (accessible) by the service provider, or retained on a centralized service or in cloud storage.

f. Device-Level Machine Learning—New machine learning focused semiconductor components and algorithms—along with the speedy, low-cost local storage and local processing capabilities of edge computing—are allowing tasks that use to require the computing horsepower of the cloud to be done in a more refined and more focused way on edge devices.

g. Identity Management—Many identity management solutions under consideration or development leverage a variety of platforms, including distributed ledger technology (described above), and local processing, that capitalize on device-level machine learning to provide the ability for individuals to verify and certify their identity. This enables people without Internet access beyond smartphones or other simple devices to form secure connections, exchange identity-related credentials (such as transcripts or voting records) without going through a centralized intermediary. Verified personal data can be accessed from the user’s device and shared via secure, encrypted channels to third parties, with data limited to the basic facts necessary for the relying party (e.g., that the individual is over 21, or does in fact qualify for a specific government service) on an as-needed basis. Depending on the implementation and standards, identity management can create privacy risks or can be deployed to support data minimization and privacy by design and default.

Advances in Artificial Intelligence (AI) & Machine Learning (ML)

h. “Small Data”—Small data AI and machine learning systems use significantly less, or even no real data, via techniques such as data augmentation (manipulating existing data sets), transfer learning (importing learnings from a pre-existing model), synthetic data sets (see below), and others. With small data techniques, the future forms of AI might be able to operate without needing the tremendous amounts of training data currently required for many applications. This capability can greatly reduce the complexity and privacy risks associated with AI and ML systems.

i. Synthetic Data Sets—Synthetic data sets are sets of artificial data created to replicate the patterns and analytic potential of real data about real individuals or events by replicating the important statistical properties of real data. They can be created at a vast scale and reduce the need for large training or test data sets, particularly for AI and ML applications, and thus support reduced data sharing or secondary use concerns.

j. Generative Adversarial Networks—Generative Adversarial Networks (GANs) are a type of artificial intelligence, where algorithms are created in pairs (one to “learn,” and the other to “judge”). Used in unsupervised machine learning, two neural networks contest with each other in a framework to produce better and better simulations of real data (creating faces of people, or handwriting). One valuable use: generating synthetic data sets.

These tools and resources can potentially help mitigate data protection concerns posed by future technologies. Federal legislation could incentivize the growth and development of new PETS. The market for compliance tools for privacy and security professionals also continues to accelerate. Services that discover, map, and cat-

---


egorize data for organizations, wizards that help manage and complete privacy impact assessments, programs that handle data subject access requests and consent management, and deidentification services are already supporting privacy and security professionals at leading organizations as well as attracting investor interest.\(^{56}\) Data protection resources entering the marketing are increasingly central to building systems that allow professionals to manage the challenges that accompany the expanded data collection and the multiplying uses that shape modern business practices.

### 6. Machine Learning

A Federal privacy law should also promote beneficial uses of artificial intelligence (AI) and machine learning. Many device manufacturers are making strides to minimize data collection by conducting data processing on-device (locally) rather than sending data back to a remote server. However, AI and machine learning technologies typically require large and representative data sets to power new models, to ensure accuracy, and to avoid bias. A U.S. framework would be wise to ensure that uses of data for machine learning are supported when conducted responsibly. To assess such responsible uses, we again recommend the development of a serious ethics review process. The academic IRB is well established as a necessary way for federally funded human subject research to be vetted.\(^{57}\) Counterparts for corporate data will be important, if structured to provide expertise, confidentiality, independence, transparency of process, speed, and expertise.\(^{58}\)

### 7. Interaction with Existing Legal Frameworks

A Federal baseline privacy law should take into consideration existing legal frameworks, by preempting certain state laws where they create conflicting or inconsistent requirements, and superseding or filling gaps between existing Federal sectoral laws. While recognizing the United States’ unique global privacy leadership, a Federal privacy law should also address issues of interoperability with GDPR and other global legal regimes. At a minimum, it is important for the U.S. to protect cross-border data flows by not creating obligations that directly conflict with other existing international frameworks.

#### A. Interaction with State Laws

The drafting of a Federal privacy law in the United States will necessarily impact the range of state and local privacy laws that have been passed in recent decades or are currently being drafted. The question of preemption is at the forefront of many conversations regarding a Federal privacy bill. Stakeholders from government, industry, civil society, and academia have expressed strong and sometimes conflicting views. At a minimum, we should seek to avoid a framework where website operators are expected to comply with multiple inconsistent state mandates on the many day-to-day issues at the core of the digital economy, ranging from signing users up for e-mail lists, implementing website analytics, or conducting e-commerce. These concerns can reasonably be avoided with carefully crafted Federal preemption, so long as the law also ensures a strong level of uniform privacy protections, certainly meeting and exceeding the core protections of the California Consumer Privacy Act (CCPA).

It is important to recognize that lawmakers’ options are not binary. The choice is not between a preemptive Federal law and a non-preemptive Federal law. Rather, lawmakers must grapple with a range of state authorities and choose which to preempt and which to preserve.\(^{59}\) I provide further context below. My core recommendations are that Congress: (1) preserve state Unfair and Deceptive Acts and Practices (UDAP) laws, which regulate a wide range of commercial conduct, from fair pricing to honest advertising, when they do not specifically target privacy or security requirements; (2) preempt generally applicable consumer privacy laws, like the California Consumer Privacy Act (CCPA); and (3) be thoughtful about which state sectoral privacy laws to preempt or preserve.

---


For example, to the extent that a Federal law contains provisions that conflict with state common law or statutes, the latter will be preempted by default.60 Congress may, to the extent it wishes, take further steps to prevent states or local governments from drafting further new, different, or more protective laws, through express or implied “field preemption.” Within this range, there is great flexibility in the extent to which a Federal law can have preemptive effect.61

As this Committee considers the appropriate balance of Federal and state intervention in the field of information privacy, it should carefully consider how a Federal privacy law will impact certain key aspects of current state regulation:

- **State UDAP Laws.** Every state has broadly applicable Unfair and Deceptive Acts and Practices (UDAP) laws that prohibit deceptive commercial practices or unfair or unconscionable business practices.62 State enforcement authorities have increasingly applied UDAP laws to data-driven business practices such as mobile apps and platform providers.63 In general, states should maintain the freedom to enforce broadly applicable commercial fairness principles in a technology-neutral manner, to the extent that they do not specifically regulate the collection and processing of personal information addressed in the Federal law.

- **State Constitutions.** Eleven states have enumerated constitutional rights to privacy, most of which were created through constitutional amendments in the last 50 years.64 In addition to governing law enforcement access to information, some states have chosen to express a free-standing fundamental right to privacy.65 These amendments to state constitutions reflect the states’ explicit intention to extend—or clarify—the fundamental rights of their own residents beyond the existing status quo of Federal legal protections.

- **State Sector-Specific Laws.** Comprehensive state efforts to regulate consumer privacy and security, such as generally applicable data breach laws or the recent California Consumer Privacy Act, are likely to be partially or fully preempted by a Federal law that meaningfully addresses the same issues and creates similar substantive legal protections. However, a Federal law should also carefully anticipate its effect on sectoral state efforts, such as those regulating biometrics,66 drones/UAV,67 or employer or school ability to ask for social media credentials.68 For example, in the field of student privacy, more than 120 state laws have passed since 2013 regulating local and state education agencies and education technology companies,69 and replacing those laws with a general consumer privacy law could eliminate important nuances that those laws incorporated; for example, a consumer privacy law would likely allow for users to delete their data, but, in the education context, students obviously should not have the ability to delete a homework assignment or test scores. Further complicating these matters, states retain a constitutional right to regulate the core

---

60 Supremacy Clause, U.S. CONST. art. VI, cl. 2.
66 Biometric Information Privacy Act (BIPA), 740 ILCS/14 (2008).
behavior of their own governmental entities, including the regulation of school districts. 70

B. Interaction with Federal Sectoral Laws

In some cases, it may be appropriate for a baseline, comprehensive Federal privacy law to supersede and replace existing sectoral Federal laws where a consistent baseline set of obligations would be beneficial. In other cases, the wide range of existing sectoral laws, including privacy laws and anti-discrimination laws, may be well suited to address concerns around automated decision-making or unfair uses of data.

C. Interaction with Global Privacy Frameworks

The U.S. has an opportunity to demonstrate leadership, protect consumers, and facilitate commerce by crafting a Federal privacy law that ensures interoperability with international data protection laws. Just as the U.S. is currently confronting challenges posed by an assortment of privacy-focused state laws, disparate privacy regimes with varying degrees of privacy protections and controls are proliferating internationally. These laws and the corresponding multiplicity of compliance obligations adversely affect cross-border data flows and the multinational businesses that rely on such flows to remain competitive.

Legislation should consider and address, as much as possible, interoperability with other nations’ privacy frameworks. 71 For example, legislation should promote interoperability with the most well-known example of a comprehensive privacy law, GDPR, which provides an extensive framework for the collection and use of personal data. The basic principles of GDPR should provide a reference for policymakers during the legislative process, with an understanding that the U.S. approach to privacy and other constitutional values may diverge in many areas, such as breadth of data subject rights, recognition of First Amendment rights, and the need for minimization requirements that may impact data use for AI and machine learning purposes. Also important for comparison are the OECD privacy guidelines and the APEC CBPR system as a valid data privacy compliance mechanism for data-transfers between the countries.

A Federal baseline privacy law should also promote cross-border data flows by avoiding the creation of obligations that directly conflict with other international laws. For example, an emergence of recent data localization laws have expressly prohibited data transfers or mandated highly-restrictive regulatory environments, resulting in inefficient and burdensome requirements for activities including: data storage, management, processing, and analytics. Countries that erect these barriers to data flows often cite concerns about cybersecurity, national security, and privacy. 72 Localization detrimentally impacts businesses, 73 consumers who benefit from free flows of data, and potentially data security. Thoughtful data governance and oversight policies with data subject rights and other protections can address data

---

protection issues without resorting to a regulatory environment that employs localization as a solution.

8. Rulemaking, Civil Penalties, and Enforcement

No matter how well crafted, a privacy law will almost certainly require a well-resourced administrative mechanism to clarify certain terms and standards. In Europe, the GDPR contemplates that guidance from Data Protection Authorities will clarify key concepts and requirements. In California, the CCPA tasks the state attorney general with promulgating rules on complicated aspects of the statute. Under Federal law, Congress provided for the FTC to issue regulations under the COPPA statute that have helped define key provisions and enable the law’s safe-harbor program for the collection and use of children’s data.

A comprehensive Federal privacy law is no different. I urge the Committee to carefully consider what aspects of a Federal law might benefit from regulatory clarity or guidance over time. And I urge legislative drafters to empower the FTC to provide such clarity, with specific parameters and considerations to take into account and subject to reasonable guardrails on the agency’s authority. The Commission and other stakeholders have agreed, and noted that additional investigatory resources would be welcome. The Commission receives many consumer complaints and would benefit from the ability to hire more technology and legal experts. Enhanced resources, and the deeper understanding of technology and business practices they bring to the Commission, can lead to fairer outcomes for both individuals and companies.

The authority to bring civil penalties is another key aspect of the FTC’s current oversight of global technology firms. But today, the FTC can only fully exercise this oversight regarding companies with whom the Commission has entered into settlement agreements. Civil penalty authority in the first instance would enable the FTC to bring its oversight to bear on all companies that handle personal data, protecting individuals and consumers and leveling the playing field.

It is also vital that technical assistance be provided if a new law is passed, particularly for small businesses. The FTC can help fulfill this role. A potential model for this is the U.S. Department of Education’s Privacy Technical Assistance Center (PTAC), which has played a vital role in providing guidance, technical assistance, and best practices to states, districts, companies, and privacy advocates. 74

Finally, there has also been a growing recognition of the important role of state attorneys general in the creation and protection of evolving privacy norms. 75 State attorneys general have brought enforcement actions that meaningfully push forward legal protections in many areas. 76 As officials with a broad scope of authority and the freedom to respond to rapidly evolving privacy challenges, they should remain key partners in the enforcement of a baseline Federal information privacy law.

Conclusion

This is a critical juncture for U.S. policymaking. Privacy regulation is charging ahead in the EU and in the states. Now is the time for the United States as a nation to reassert its policy leadership, which stretches from Warren and Brandeis’ 1890 treatise on The Right to Privacy, 77 through William Prosser’s explication of the privacy torts in 1960, 78 to the Department of Health, Education, and Welfare’s report first outlining the fair information practices in 1972, 79 which are the cornerstone for every data protection framework from OECD to GDPR.

Federal legislation should empower the FTC to rulemake and enforce and allow state AGs to retain enforcement powers. It should recognize broad spectrum of identifiability in definition of PII. It should provide heightened protection for sensitive data or contexts. It should not unduly restrict socially beneficial research find a way

---

77 Id.
to enable crucial data-driven research. It should incentivize and recognize the privacy profession and PETs.

In my view, the best approach would be for Congress to draft and pass a baseline, non-sectoral Federal information privacy law. Although I have flagged specific considerations related to such a law's content and its interaction with existing legal frameworks, I overall believe that a strong Federal law remains the best approach to guaranteeing clear, consistent, and meaningful privacy and security protections in the United States.

APPENDED:
A. Future of Privacy Forum, Infographic, Personal Data and the Organization: Stewardship and Strategy
C. Future of Privacy Forum Infographic, Financial Data Localization: Conflicts and Consequences
D. Future of Privacy Forum, Draft Legislative Language: “Covered Data”
E. Future of Privacy Forum, Unfairness by Algorithm: Distilling the Harms of Automated Decision-making (December 2017)
F. Future of Privacy Forum & Anti-Defamation League, Big Data: A Tool for Fighting Discrimination and Empowering Groups

The CHAIRMAN. And thank you very much, sir.

Mr. Steyer.

STATEMENT OF JAMES P. STEYER, CHIEF EXECUTIVE OFFICER AND FOUNDER, COMMON SENSE MEDIA

Mr. Steyer. Thank you, Chairman Wicker, Ranking Member Cantwell, and the distinguished members of this Committee. It is great to be here.

I am Jim Steyer. I am the Founder and CEO of Common Sense Media. We are the leading kids’ media and tech group in the United States. We launched about 15 years ago. Just for a little background, we have 110 million unique users every year on our consumer platform. We created an award-winning digital citizenship curriculum that is in most of the schools in your guys’ states. And we have 75,000 member schools across the world, most of which are in the U.S., teaching kids about not just their privacy rights but the safe, responsible use of tech.

I am also a prof at Stanford where I have taught constitutional law for the last 30 years.

The one thing I would sort of say in general today is that as someone who has been a child advocate for 30 years—I am a father of four. I have got a 15-year-old. That is our youngest now. I think this is a major moment in time on these issues. It has been literally almost 20 years since the U.S. Congress did anything meaningful in the area of privacy. And right now, even though there are tens of millions of American families who are worried about privacy issues for themselves, but most of all for their children, there is only one state, the state that I live in, California, that has a comprehensive privacy law. And in fact, it was us at Common Sense Media who spearheaded that law last year, the CCPA that has been referred to.

I just think it is this great moment in time where this body has to act. I always say when I get up in front of parents that 20 years ago Mark Zuckerberg was barely out of diapers. Google was a concept in sort of obscure math ideas. And this device did not even exist. But it is all here now and our kids are living on it and we are all living on it. And so during this time of extraordinary growth...
in the tech economy, we have got to come up with a comprehensive, smart, common sense privacy law that is going to protect all of us, all of our families, and most of all, our kids.

Right now, there essentially are no guardrails when it comes to privacy federally. We have one law, the California law that we passed last year. It goes into effect in January. And then we have GDPR, which Ms. Dixon referred to. So it is high time that Congress and this august body stepped up to the plate and protected the fundamental privacy rights of every citizen in this country.

The one thing that we saw very much in California when we passed the law is that it is a totally bipartisan issue. This is something that everybody ought to be able to agree on because we all are both the beneficiaries of the extraordinary aspects of the tech industry, but we are also the victims when privacy rights are violated, whether it is individually or whether it involves interference with our electoral process. So overwhelming majorities of Americans agree with us. The California law passed unanimously. And so I would just urge you to really work, as you do, as a bipartisan group to support comprehensive privacy laws now.

Four big points that I would say to you.

One, the California law is a floor, not a ceiling. Anything that should come out of this committee and this Senate should be stronger than the California law. I know. We negotiated it. We gave up a number of rights in order to get it passed. We worked with companies like Microsoft, Apple, and Salesforce to get it done. But this body should be looking at California as an absolute floor rather than as a ceiling.

The second thing I would say is that kids and teens are the most vulnerable. They deserve special protection. As our good friend, Senator Markey, knows as well as anyone, kids need extremely important and unique protections. So as you consider the law, we hope you will put kids first and include teens in this law as well.

Third, there needs to be ongoing public education, a public awareness campaign. The average American, I would argue the average Senator, is not a computer wizard or tech wizard. So once we have a law, we need to explain it to the public how to use it. That is a big thing we are going to start doing in California in 2020. But I would urge you to think about that, how do you make it simple, easy, and easily understandable for a luddite like me and some of you.

And last but not least, I do want to raise the other thing. In the wake of the live streaming of mass shootings on Facebook a few weeks ago, and the inability of YouTube and other platforms to pull some of that extraordinarily inappropriate content for anyone, let alone children, down, we would urge you to think about it separately, the concept of section 230 in the safe harbor provision and what kind of regulations there ought to be, for kids in particular, of inappropriate content on the Web.

At the end of the day, I think the bottom line is clear. This is your folks’ moment to do something great for everybody in America on a bipartisan basis, and we are happy to help.

Thank you very much for having me.

[The prepared statement of Mr. Steyer follows:]
PREPARED STATEMENT OF JAMES P. STEYER, CHIEF EXECUTIVE OFFICER AND FOUNDER, COMMON SENSE MEDIA

Good morning Chairman Wicker, Ranking Member Cantwell, and distinguished Committee Members. Thank you for the opportunity to appear before you, and for your willingness to engage with the complicated—but critically important—issue of consumer privacy.

My name is James P. Steyer and I am the founder and CEO of Common Sense Media. Common Sense is America’s leading organization dedicated to helping kids and families thrive in a rapidly changing digital world. We help parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids’ lives. Since launching 15 years ago, Common Sense has helped millions of families and kids think critically and make smart, responsible choices about the media they create and consume. Common Sense has over 108 million users and our award-winning Digital Citizenship Curriculum is the most comprehensive K–12 offering of its kind in the education field; we have over 700,000 registered educators using our resources in over half of U.S. schools. Common Sense was a sponsor of California’s precedent-setting consumer privacy law, the California Consumer Privacy Act (CCPA). We have also sponsored and supported privacy laws across the country and at the Federal level, including California’s landmark Student Online Privacy Information Protection Act (SOPIPA) and the recently introduced bipartisan COPPA 2.0.

Children And Teens Are Particularly Vulnerable

When we started Common Sense a decade and a half ago, privacy was not a major concern for kids and families. But it has grown significantly as an issue over the past several years, to the point where we find ourselves today. Privacy concerns are particularly acute for kids: Ninety-eight percent of children under 8 in America have access to a mobile device at home.¹ American teens consume an average of 9 hours a day of media,² and half of teens report feeling addicted to their devices. Children today face surveillance unlike any other generation—their every movement online and off can be tracked by potentially dozens of different companies and organizations. Further, kids are prone to sharing and impulsive behavior, are more susceptible to advertising, and are less able to understand what may happen to their personal information.³

Unfortunately, too many companies are not protecting children’s and their families’ privacy. A recent analysis found that more than half of 6,000 free children’s apps may serve kids ads that violate COPPA.⁴ 60 percent of connected devices don’t provide proper information on how they collect, use and disclose users’ personal information.⁵ Millions of kids and parents have had sensitive information—including family chats—exposed by connected toys.⁶ Data brokers are selling profiles of children as young as two (and identity theft can occur before a child’s first birthday).⁷

A growing lack of privacy and distrust of the online and tech world impacts every family, and could significantly impact the personal development of young people. At Common Sense, we believe kids need the freedom to make mistakes, try new things, and find their voices without the looming threat of a permanent digital record that could be used against them.

It is our goal to help our millions of American members improve the digital wellbeing of their families—and while in many instances that means teaching parents, teachers, and kids good digital citizenship practices and privacy skills, it also means ensuring there are baseline protections in place. Even savvy digital citizens are powerless if they do not know what companies are doing with their information, if they cannot access, delete, or move their information, or if they have no choices with respect to the use and disclosure of their information.

¹ Common Sense: Technology Addiction: Concern, Controversy, and Finding Balance (2016)
² Ibid
³ Children, Adolescents, and Advertising (2006)
⁴ Reyes et. al, “Won't Somebody Think of the Children?” Examining COPPA Compliance at Scale, Proceedings on Privacy Enhancing Technologies (2018)
⁵ GPEN Privacy Sweep on Internet of Things (2016)
⁷ Ibid
Families’ Privacy Expectations And Desires

What do families want in privacy protections? According to our research: More than 9 in 10 parents and teens think it’s important that websites clearly label what data they collect and how it will be used.9 Those same numbers—more than 9 in 10—think it is important that sites ask permission before selling or sharing data.9 And almost 9 in 10, or 88 percent, think it is important to control whether data is used to target ads across devices.10 Speaking of devices, 93 percent of parents believe that with smart devices it is important to control what information is collected about them and to know when their voices are being recorded.11

These views and data points informed the values—including consent, transparency, control, plus special protections for young people—that guided our approach to the privacy work we did in California.

The California Consumer Privacy Act (CCPA)

The CCPA is the first generally applicable consumer privacy law in America—not limited to financial or health information, or any specific entity—that recognizes that Americans have privacy rights in all of their information, no matter who holds it. Importantly, the California privacy law protects everyone, not just kids or students. This is born of our belief that, while children and teens need special safeguards, the best way to protect them is to have baseline protections for everyone: (1) so families are protected and (2) so businesses cannot pretend they are not dealing with kids.

In California, a statewide ballot initiative focused on notice and saying no to sales of data was the catalyst that led to larger discussions to develop more comprehensive privacy legislation. At Common Sense, we worked hard to expand substantive rights under the law—including opt-in rights (which we achieved for minors under 16), and new access, deletion, and portability rights. The CCPA ultimately passed unanimously through both houses of the California legislature.

The law goes into effect in 2020, and will allow California residents to access the personal information companies collect about them—as well as port their data to another platform, or demand the deletion of their data (with exceptions) if they wish. Californians will be empowered to tell companies to stop selling their personal information. And kids under 16 or their parents must actively consent before their data is ever sold. The Attorney General is charged with enforcing violations of the law—with a private right of action for certain data breaches—and the law applies equally to service providers, edge companies, and brick and mortar entities.

Any Federal Law Should Build Upon California

Like the CCPA, any Federal law must go beyond “consent”, and include rights to access, port, and delete information. It must enable consumers to say no to the sharing of their information. And it would be even better if the law required that consumers say yes before their information is sold or shared—families would be better served if the rule for all people, not just minors under 16, was that companies could not sell information without opt-in approval. Indeed, the California law is a huge step forward, but it is not perfect and it does not offer consumers all of the protections they deserve. As this committee considers bipartisan Federal legislation, additional protections families want and deserve include: the rights to limit companies’ own use of consumer information; the ability for consumers to enforce their own rights in court; and the assurance that companies are building default privacy protections (privacy by design) and practicing data minimization. Certain practices should be off limits, and individuals, especially children, should not be able to consent to them (such as, for example, manipulative user designs that subvert user autonomy, or behaviorally targeted marketing to kids).

Privacy protections must be strong across the board, but they must recognize the unique vulnerabilities of children and teenagers. The bipartisan COPPA 2.0 offers an excellent example of the protections young people need: in addition to putting families in the driver’s seat regarding information collection, use, and disclosure, COPPA 2.0 contains additional safeguards (and, for young children, flat prohibitions) around targeted and behavioral marketing; it would enhance the privacy and security of vulnerable connected devices families are bringing inside their homes; and it offers new resources and authority to the Federal Trade Commission to focus on examining the industry and enforcing these protections.

---

10 Ibid
11 Ibid
Any law Congress passes should be at least as strong, if not stronger, than California’s CCPA. The CCPA will go into effect next year, and it is clear from polling that vast majorities of Californians from all parties support it. What’s more, it is also clear from other states that individuals and state legislators are not going to accept laws that are weak on privacy. And, as with past Federal privacy laws, national legislation should ensure that there are baseline protections in place, but provide room and space for states to continue to innovate. A weak preemptive law would be a travesty of justice and take away rights from millions of consumers, not just the eighth of the country that lives in California but the many individuals who live in other states with strong privacy laws such as Illinois, with its biometric law, or Vermont, with its data broker registry.

States have always been the first line of defense to protect individual citizens from scams and unfair business practices, and state tort law has protected the privacy of homes and persons. State innovation in the privacy sphere has brought us data security rules, laws applying directly to ed tech vendors, laws protecting the privacy of our bodies, and laws shining light on data brokers. The speed of technology is lighting fast, and states are in a position to act nimbly and innovate, just like businesses. States are true laboratories of democracy, and in the past few decades they have been engaging on privacy and working with consumers and businesses to determine workable new protections and safeguards.

Any Law Must Be Coupled With Consumer Education

It is critical that any new law be coupled with effective consumer education. From our research at Common Sense, we know that families crave better privacy protections. We also know that some are taking measures to try and protect themselves—for example, 86 percent of parents and 79 percent of teens have adjusted privacy settings on social media sites. But in many instances, families have the desire but lack the knowledge. In discussing connected devices with parents, we learned 71 percent would like to limit data collection, but a full third do not know how.

This is why it is important to have companies build products, platforms and services with the most protective privacy defaults possible. It is also why kids and adults need to know how to exercise their privacy rights. Education is imperative in this regard. As I mentioned, Common Sense is committed to giving parents and teachers the information they need to make informed choices about the apps they use with their children at home and the learning tools they use with students in the classroom. We provide expert advice articles and privacy evaluations for parents to learn more about how they can protect their kids’ privacy and we empower schools and districts to thoroughly assess technology products used in K–12 classrooms. We collaborate with hundreds of school and district partners and provide assistance to software developers to make sure their privacy practices are transparent and comprehensive and created with kids’ best interests in mind. We also provide a high-quality Digital Citizenship Curriculum for school communities that supports teachers with improved classroom tools, and prepares kids to take ownership of their digital lives.

At present, across the country, opportunities to empower individuals to make real decisions or protect their privacy are few and far between. Companies offer a “take it or leave it” framework that, because of jobs, school requirements, or an interest in participating in democratic life, individuals feel forced to accept. We must ensure consumers have default protections in place, and we must also work to educate them about additional, or alternative, choices. Digital citizenship education should be a part of school curriculums, and requires more support and funding.

What’s more, privacy protections are just one piece of the puzzle. As young people live more and more of their lives online, they face an ever expanding array of opportunities and risks. In addition to protecting children and families’ privacy, we must endeavor to provide all kids with access to high quality content, and protect them from being exposed to the worst of humanity with the click of a button, scroll of a feed, or failure to stop a new video from autoplaying. We must consider, as a country, whether laws like Section 230 are serving the best interest of our children, and what we can do to improve the entirety of their digital experience.


—Ibid
Conclusion

Thank you again for your bipartisan efforts to address consumer privacy. It’s critical that we teach individuals how to protect themselves, but the burden should not fall entirely on consumers, especially on kids and families. We have seen many businesses will not protect consumer privacy on their own. We need a strong Federal baseline privacy law, that offers everyone protections and recognizes the special vulnerabilities of children and teens.

The CHAIRMAN. Thank you very much, Mr. Steyer.
Ms. Guliani.

STATEMENT OF NEEMA SINGH GULIANI, SENIOR LEGISLATIVE COUNSEL, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION

Ms. GULIANI. Thank you for the opportunity to testify today on behalf of the ACLU.

We are all here because the current privacy regime is broken and it is failing consumers. Lack of privacy affects everyday life. It can increase unfair discrimination, exacerbate economic inequality, and even threaten physical safety.

For example, studies have documented how some retailers charge customers different prices based on things like their Zip code or their browsing habits. In many cases, consumers are not even aware their information is being collected, much less how they can protect themselves against these types of uses.

In another study, online mortgage lenders charge black and Latin borrowers more and higher rates for their loans, replicating the types of discrimination that Federal laws like the Equal Credit Opportunity Act were designed to prevent.

The ACLU strongly supports Federal privacy legislation to address problems like these. There are many elements that such legislation should include, but I want to highlight four areas in particular that are of concern.

The first is any Federal law should be a floor, not a ceiling. Some industry representatives have urged you to broadly preempt State laws as part of any Federal legislation. I want to be crystal clear here. This would be a bad deal for consumers. If Congress uses Federal privacy legislation as an opportunity to broadly preempt State laws, it will cause more harm than good.

As an organization with affiliates in every state, the ACLU has been at the forefront of many efforts to pass strong State privacy laws. We know firsthand that in many cases it has been states, not Congress, that have led efforts to protect consumers. California was the first State in the Nation to require companies to notify customers of a data breach, and just last year it passed a broader consumer privacy bill that you all are familiar with.

Illinois has set important limits on the commercial collection and storage of biometric information, and nearly all states regulate unfair and deceptive trade practices, complementing the FTC’s authority in this area.

These states have acted as laboratories. They have experimented and innovated with new ways to protect consumers. We should be wary of the Federal Government stepping in and with one stroke of a pen wiping out dozens of State laws already on the books and preventing future ones.
Broad preemption, in fact, would represent a shift in the approach taken by many Federal laws. HIPAA allows states to enact more stringent privacy protections for health information, and Federal civil rights laws have historically allowed states to pass higher standards. This is one of the reasons we have State laws that protect against discrimination on the basis of sexual orientation, despite the gaps in Federal law.

Federal legislation must certainly account for cases where it would be impossible to comply with both a State and Federal law. But that can be accomplished through a narrow and clear preemption provision that addresses conflicts and explicitly preserves the rights of states to pass stronger laws and to enforce those laws.

Two, any privacy legislation should allow consumers to sue companies that violate their rights. The FTC undoubtedly needs more power and more resources. But even if its size were doubled or even tripled, there would be giant enforcement gaps. This is part of the reason that the California Attorney General recently supported legislation to strengthen California’s law with a privacy right of action. In discussing the legislation, he said, quote, we need to have some help. He highlighted that individuals should be able to enforce their rights in cases where the government was not able to take action. Polling in California has found that 94 percent of consumers support being able to take a company to court if their privacy rights are violated.

Three, legislation should protect against discrimination. There must be the resources and the technical expertise to enforce existing Federal laws that prohibit discrimination in the housing, credit, and employment context.

In addition, however, Federal law must be strengthened to prohibit advertisers from offering different price, services, and opportunities to individuals based on protected characteristics like race and gender.

And consumers must also have the tools to address algorithms or machine learning tools that disparately impact individuals on the basis of such protected characteristics.

Finally, there should be guardrails on how data can be collected, stored, and used. For example, use of information should be limited to the purpose for which it was collected unless there is additional informed consent. And we should also prohibit so-called pay for privacy schemes that threaten to create privacy haves and have-nots and risk causing disastrous consequences for people who are already struggling financially.

Without these protections a new Federal law risks being a step backward, not forward.

I look forward to answering your questions.

[The prepared statement of Ms. Guliani follows:]
Chairman Thune, Ranking Member Cantwell, and Members of the Committee,

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU)\(^1\) and for holding this hearing on, “Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework.”\(^2\)

Privacy impacts virtually every facet of modern life. Personal information can be exploited to unfairly discriminate, exacerbate economic inequality, or undermine security. Unfortunately, our existing laws have not kept pace with technology, leaving consumers with little ability to control their own personal information or recourse in cases where their rights are violated. And, as numerous examples illustrate, consumers are paying the price. Studies have documented how several retailers charged consumers different prices by exploiting information related to their digital habits inferred from people’s web-browsing history.\(^2\) Some online mortgage lenders have charged Latino and Black borrowers more for loans, potentially by determining loan rates based on machine learning and patterns in big data.\(^3\) And, sensitive data about the location and staffing of U.S. military bases abroad was reportedly revealed inadvertently by a fitness app that posted the location information of users online.\(^4\)

The current privacy landscape is untenable for consumers. The ACLU\(^1\) supports strong baseline Federal legislation to protect consumer privacy. I would like to emphasize several issues that are of particular concern to the ACLU and our members. The ACLU strongly urges Congress to ensure that any Federal privacy legislation, at a minimum, (1) sets a floor, not a ceiling, for state level protection; (2) contains robust enforcement mechanisms, including a private right of action; (3) prevents data from being used to improperly discriminate on the basis of race, sexual orientation, or other protected characteristics; and (4) creates clear and strong ground rules for the use, collection, and retention of consumers’ personal data, which does not rest solely on the flawed notice and consent model.

I. Federal legislation should not prevent states from putting in place stronger consumer protections or taking enforcement action

Any Federal privacy standards should be a floor—not a ceiling—for consumer protections. The ACLU strongly opposes legislation that would, as some industry groups have urged, preempt stronger state laws.\(^5\) Such an approach would put existing consumer protections, many of which are state-led, at risk. It would prevent additional consumer privacy protections from ever seeing the light of day. We also oppose efforts to limit the ability of state Attorneys General or other regulators from suing, fining, or taking other actions against companies that violate their laws.

There are multiple examples of states leading the charge to pass laws to protect consumer privacy from new and emerging threats. For example, California was the first state in the Nation to require that companies notify consumers\(^6\) of a data breach (all states have since followed suit),\(^7\) the first to mandate that companies disclose through a conspicuous privacy policy the types of information they collect and

---

\(^1\) For nearly 100 years, the ACLU has been our Nation’s guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than three million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.


\(^6\) See California Civil Code s. 1798.25–1798.29.

share with third parties,\(^8\) and among the first to recognize data privacy rights for children.\(^9\) The state's recently passed California Consumer Privacy Act of 2018, which goes into effect next year, is also the first in the Nation to apply consumer protections to a broad range of businesses, including provisions that limit the sale of personal information, give consumers the right to delete and obtain information about how their data is being used, and provide a narrow private right of action for some instances of data breach.

Similarly, Illinois has set important limits on the commercial collection and storage of biometric information, such as fingerprints and face prints.\(^10\) Idaho, West Virginia, Oklahoma, and other states have passed laws to protect student privacy.\(^11\) Nevada and Minnesota require Internet service providers to keep certain information about their customers private and to prevent disclosure of personally identifying information.\(^12\) Arkansas and Vermont have enacted legislation to prevent employers from requesting passwords to personal Internet accounts to get or keep a job. At least 34 states also require private or governmental entities to conduct data minimization and/or disposal of personal information,\(^13\) and 22 have laws implementing data security measures.\(^14\)

Historically, states have also served a critical enforcement role in the consumer space, as illustrated by the recent Equifax breach. As a result of that breach, the data of over 140 million consumers were exposed due to what some members of Congress referred to as "malfeasance" on the part of the company.\(^15\) Despite this, the company posted record profits the following year, and consumers have still not been fully compensated for the cost of credit freezes the breach made necessary. While the FTC has an ongoing investigation, it has yet to take action. In the meantime, the Massachusetts attorney general is currently suing Equifax seeking damages in an attempt to obtain compensation for individuals impacted by the breach. In addition, several state regulators have entered into a consent decree with the company that puts in place new requirements.\(^16\)

States have been and will continue to be well-positioned to respond to emerging privacy challenges in our digital ecosystem. New technology will likely require additional protections and experimenting with different solutions, and states can serve as laboratories for testing these solutions. Thus, we should avoid preemption that could lock in place Federal standards that may soon be obsolete or prevent states from fully utilizing their enforcement capabilities.

Preemption would not only be bad for consumers, it would represent a shift in the approach taken by many of our existing laws. For example, the Telecommunications Act explicitly allows states to enforce additional oversight and regulatory systems for telephone equipment, provided they do not interfere Federal law; it also permits states to regulate additional terms and conditions for mobile phone services. Title I of the Affordable Care Act permits states to put in place additional consumer protections related to coverage of health insurance plans, and HIPPA similarly allows states to enact more stringent protections for health information.

In addition, all 50 states in some way regulate unfair or deceptive trade practices, an area also governed by section 5 of the FTC Act.\(^17\) While the strength of these state laws vary, they are harmonious with the FTC's mandate and are integral to
manageable privacy regulation enforcement. Such coordination has historically allowed states to fill gaps that Federal regulators simply do not have the resources or expertise to address. (An Appendix of additional state privacy laws is attached to this testimony.)

We recognize that any Federal legislation must account for conflicts in cases where it would be impossible for an entity to comply with both Federal and state laws. However, this can be accomplished through a clear, narrow conflict-preemption provision, which explicitly preserves stronger state laws that do not undermine Federal standards, maintains state enforcement capabilities, and retains state consumer remedies.

II. Federal legislation must contain strong enforcement mechanisms, including a private right of action

Federal privacy legislation will mean little without robust enforcement. Thus, any legislation should grant greater resources and enforcement capabilities to the FTC and permit state and local authorities to fully enforce Federal law. To fill the inevitable enforcement gaps, however, the ACLU urges Congress to ensure that Federal legislation also grants consumers the right to sue companies for privacy violations.

The FTC has a long history of protecting consumer privacy in the United States. But, alone and with current resources and authorities, it cannot effectively police privacy alone. In the last 20 years, the number of employees at the FTC has grown only slightly. And the number of employees in the Division of Privacy and Identity Protection (DPIP) and the Division of Enforcement, which are responsible for the agency’s privacy and data security work, stands at approximately 50 and 44 people, respectively. To put this in perspective, this is smaller than the Washington, D.C. offices of many large technology companies alone. Both the FTC as a whole and DPIP require additional resources and employees to address the outsize risks to privacy facing consumers.

And for the agency’s investigations and enforcement actions to have meaningful deterrent effect, the FTC should be given authority to levy significant civil penalties in consumer protection actions for the first violation, rather than only in cases where a company is already under a consent decree. It was recently announced that Facebook has set aside 3 to 5 billion dollars to pay a potential fine to the FTC for its mishandling of personal information, including conduct related to Cambridge Analytica. Following this announcement, Facebook’s stock value surged nonetheless, suggesting that the FTC’s current enforcement powers are woefully lacking when measured against the earning potential of the largest online businesses.

To augment the limited Federal enforcement resources, state and local enforcement entities should also be given the power to investigate and enforce Federal privacy law. This aligns with the approach taken by other laws, including the Fair Debt Collection Practices Act, which is enforceable by state Attorneys General as well as through a private right of action. Government enforcement will inevitably have gaps. Thus, providing consumers a private right of action under the [California Consumer Privacy Act].

The FTC has a long history of protecting consumer privacy in the United States. But, alone and with current resources and authorities, it cannot effectively police privacy alone. In the last 20 years, the number of employees at the FTC has grown only slightly. And the number of employees in the Division of Privacy and Identity Protection (DPIP) and the Division of Enforcement, which are responsible for the agency’s privacy and data security work, stands at approximately 50 and 44 people, respectively. To put this in perspective, this is smaller than the Washington, D.C. offices of many large technology companies alone. Both the FTC as a whole and DPIP require additional resources and employees to address the outsize risks to privacy facing consumers.

And for the agency’s investigations and enforcement actions to have meaningful deterrent effect, the FTC should be given authority to levy significant civil penalties in consumer protection actions for the first violation, rather than only in cases where a company is already under a consent decree. It was recently announced that Facebook has set aside 3 to 5 billion dollars to pay a potential fine to the FTC for its mishandling of personal information, including conduct related to Cambridge Analytica. Following this announcement, Facebook’s stock value surged nonetheless, suggesting that the FTC’s current enforcement powers are woefully lacking when measured against the earning potential of the largest online businesses.

To augment the limited Federal enforcement resources, state and local enforcement entities should also be given the power to investigate and enforce Federal privacy law. This aligns with the approach taken by other laws, including the Fair Debt Collection Practices Act, which is enforceable by state Attorneys General as well as through a private right of action. Even with these reforms, however, the scale and scope of potential harm associated with poor privacy practices are too extensive to be left to regulators.

Government enforcement will inevitably have gaps. Thus, providing consumers a private right of action is also critical from an enforcement standpoint—a concept reflected in several state approaches. For example, the Illinois Biometric Information Privacy Act permits aggrieved individuals whose rights are violated to file suit to seek damages in several state approaches. For example, the Illinois Biometric Information Privacy Act permits aggrieved individuals whose rights are violated to file suit to seek damages in several state approaches.
Privacy law should neither tolerate such waivers nor indulge the legal ‘effective access to justice’ for those encountering diverse violations of their legal rights.”

In order to be effective, a private right of action should have two key protections for consumers. First, it should specify statutory damages for all violations of privacy rights, not just instances where a consumer has offered conclusive proof of tangible damages. When conduct is potentially harmful, statutory damages offer a compelling solution. In copyright infringement, for example, statutory damages can range from $750 to $30,000 per work infringed. Similarly, the Fair Debt Collection Practices Act provides for statutory damages of up to $1,000 per violation. These statutory-damage provisions encourage rigorous compliance by establishing that violations carry a significant penalty. Privacy law should do the same.

Second, consumers should be protected against mandatory arbitration clauses buried in terms of service that restrict their rights to have a court hear their claims and undermine the ability of class actions to collectively redress privacy violations.

One Federal judge called these arbitration clauses "a totally coerced waiver of both the right to a jury and the right of access to the courts" that are "based on nothing but factual and legal fictions." Similarly, in a dissent in this term’s Lamps Plus case, Justice Ginsburg noted, "mandatory individual arbitration continues to thwart ‘effective access to justice’ for those encountering diverse violations of their legal rights.” Privacy law should neither tolerate such waivers nor indulge the legal and factual fictions that underlie them.

III. Federal legislation should guard against discrimination in the digital ecosystem

Existing Federal laws prohibit discrimination in the credit, employment, and housing context. Any Federal privacy legislation should ensure such prohibitions apply fully in the digital ecosystem and are robustly enforced. In addition, we urge Congress to strengthen existing laws to guard against unfair discrimination, including in cases where it may stem from algorithmic bias.

Many online providers have been slow to fully comply with Federal antidiscrimination laws. The rise of big data and personalized marketing has enabled new forms of discrimination that run afoul of existing Federal laws, including Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Equal Credit Opportunity Act. For example, Facebook recently settled a lawsuit brought by ACLU and other civil rights organizations amid allegations that it discriminated on the basis of gender and age in targeting ads for housing and employment. The lawsuit followed repeated failures by the company to fully respond to studies demonstrating that the platform improperly permitted ad targeting based on prohibited characteristics, like race, or proxies for such characteristics. The company is also now the subject of charges brought by the Department of Housing and Urban Development (HUD), which includes similar allegations.

Outside the credit, employment, and housing contexts, discriminatory targeting and marketing may also raise civil rights concerns. For example, commercial advertisers should not be permitted to offer different prices, services, or opportunities to individuals, or to exclude them from receiving ads offering certain commercial benefits, based on characteristics like their gender or race. And regulators and con-

---

24 Biometric Information Privacy Act, supra note 10, 740 ILCS 14/, Section 20.
27 17 U.S.C. §504(c)(2).
28 15 USC 1692k.
sumers should be given information and tools to address algorithms or machine learning models that disparately impact individuals on the basis of protected characteristics. Federal law must be strengthened to address these challenges. First, Federal privacy law should make clear that existing antidiscrimination laws apply fully in the online ecosystem, including in online marketing and advertising. Federal agencies that enforce these laws, like HUD, the EEOC, and the Consumer Financial Protection Bureau, should be fully resourced and given the technical capability to vigorously enforce the law in the context of these new forms of digital discrimination. In addition, companies should be required to audit their data processing practices for bias and privacy risks, and such audits should be made available to regulators and disclosed publicly, with redactions if necessary to protect proprietary information. Finally, researchers should be permitted to independently audit platforms for bias, and Congress should not permit enforcement of terms of service that interfere with such testing.

IV. Federal privacy legislation must place limits on how personal information can be collected, used, and retained.

Legislation must include real protections that consider the modern reality of how people’s personal information is collected, retained, and used. The law should limit the purposes for which consumer data can be used, require purging of data after permissible use have completed, prevent coercive conditioning of services on waiving privacy rights, and limit so-called “pay for privacy” schemes. Otherwise, we risk ending up in the same place we began—with consumers simply checking boxes to consent with no real understanding of or control over how their data will be used. This current broken privacy regime has largely been built around the concept of “notice and consent”: as long as a company includes a description of what it is doing somewhere in a lengthy fine-print click-through “agreement,” and the consumer “agrees” (which they must do to utilize a service), then the company is broadly regarded as having met its privacy obligations. And legally, a company is most vulnerable if it violates specific promises in those click-through agreements or other advertisements. An ecosystem of widespread privacy invasions has grown out of the impossible legal fiction that consumers read and understand such agreements. The truth is that consumers do not have real transparency into how their data is being used and abused, and they do not have meaningful control over how their data is used once it leaves their hands.

Worse, technologists and academics have found that advertising companies “innovate” in online tracking technologies to resist consumers’ attempts to defeat that tracking. This is done by, for example, using multiple identifiers that replicate each other, virus-like, when users attempt to delete them. Technical circumvention of privacy protections is sufficiently commonplace that data brokers are even offering what is effectively re-identification as a service, promising the ability to “reach customers, not cookies.” Advertisers, the experts conclude, “use new, relatively unknown technologies to track people, specifically because consumers have not heard of these techniques. Furthermore, these technologies obviate choice mechanisms that consumers exercise.”

In short, not only have consumers lost control over how and when they are monitored online, companies are actively working to defeat efforts to resist that monitoring. Currently, individuals who want privacy must attempt to win a technological arms race with the multi-billion dollar Internet-advertising industry. American consumers are not content with this state of affairs. Numerous polls show that the current online ecosystem makes people profoundly uncomfortable. Similarly, recent

---

36 Reach Customers, Not Just Cookies, LiveRamp Blog, September 10, 2015 (available at https://liveramp.com/blog/reach-customers-not-just-cookies/) (“Cookies are like an anonymous ID that cannot identify you as a person.”).
to address these deficiencies, privacy legislation should include a meaningful “opt-in” baseline rule for the collection and sharing of personal information. To be meaningful, protections must not allow businesses to force consumers, in order to participate fully in society, to “agree” to arcane lengthy, agreements that they cannot understand. Legislation should also support technological opt-in mechanisms such as “do not track” flags in web browsers by requiring that companies honor those flags. In addition to this, Federal legislation should approach the collection (and especially use) of personal information that is not necessary for the provision of a service with skepticism.

Moreover, the law should reject so-called “pay-for-privacy” schemes, which allow companies to offer a more expensive or lower quality product to people who exercise privacy rights. These kinds of schemes discourage everyone from exercising their privacy rights, and risk causing disastrous follow-on consequences for people who are already financially struggling. Privacy is a right that everyone should have, not just people with the ability to pay for it.

V. Conclusion

The current Federal privacy framework is failing consumers. But, in enacting Federal privacy legislation, Congress must ensure that it does not do more harm than good by preempting existing and future state laws that protect consumers. Moreover, it must ensure that its reforms amount to more than just a fig leaf. Consumers do not need another box to check; they need limits on how companies can treat their data, the ability to enforce their privacy rights in court, and protection against digital discrimination. These reforms and others are necessary to prevent exploitation of data from being used to exacerbate inequality, unfairly discriminate, and undermine security.

APPENDIX. STATE PRIVACY LAWS

The chart below provides a list of some existing state privacy laws. This is not an exhaustive list of all state consumer privacy laws, nor does it include all general laws that may be relevant in the consumer privacy context.

<table>
<thead>
<tr>
<th>State</th>
<th>Summary and/or Relevant Provisions</th>
<th>Source</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>State</th>
<th>Summary and/or Relevant Provisions</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>Breach notification law that provides for: (1) notice requirement when a breach of security concerning personal information has occurred; (2) ability to place a security freeze on a consumer credit report; (3) various restrictions on the use of personal information and credit information; (4) disposal of records containing personal information; (5) allowing a victim of identity theft to petition the court for a determination of factual innocence; and (6) truncation of credit card information. The SSN section also states that no one can require disclosure of a SSN to access a product or service. State constitution: “The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.” Alaska Const. art. I, § 22 Unfair Trade Practices and Consumer Protection Act. Broadly prohibits unfair, deceptive, or unconscionable acts. Creates a private right of action and gives Attorney General and district attorneys power to enforce statute. When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records. Alaska Stat. §§ 45.48.500</td>
<td>Alaska Stat. Ann. §§ 45.48.010 (“Alaska Personal Information Act”)</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Requires government websites or state portals to establish privacy policies and procedures and incorporate machine-readable privacy policies into their websites. Data security law that applies to a person or business that acquires, owns, or licenses personal information. Requires implementation and maintenance of reasonable security procedures and practices appropriate to the nature of the information. Amended to include biometric data. Prevents employers from requesting passwords to personal Internet accounts to get or keep a job. Prohibits use of Automated License Plate Readers (ALPRs) by individuals, partnerships, companies, associations or state agencies. Provides exceptions for limited use by law enforcement, by parking enforcement entities, or for controlling access to secure areas. Prohibits data from being preserved for more than 150 days. Ark. Code Ann. §§ 12–12–1801 to 12–12–1808 (“Automatic License Plate Reader System Act”)</td>
<td>Ark. Code Ann. §§ 25–1–114 Ark. Code Ann. §4–110–101 to -10 (Personal Information Protection Act) amended in 2019 Arkansas Law Act 1030 (H.B. 1943) Ark. Code Ann. §§ 11–2–124 Ark. Code §§ 12–12–1801 to 12–12–1808 (“Automatic License Plate Reader System Act”)</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>California</td>
<td>Gives consumers right to request a business to disclose the categories and specific pieces of personal information that the business has collected about the consumers and the source of that information and business purpose for collecting the information. Consumers may request that a business delete personal information that the business collected from the consumers. Consumers have the right to opt out of a business’s sale of their personal information, and a business may not discriminate against consumers who opt out. Applies to California residents. Effective Jan. 1, 2020.</td>
<td>Cal. Civ. Code § 1798.100 to .198 (&quot;The California Consumer Privacy Act of 2018&quot;)</td>
</tr>
<tr>
<td></td>
<td>State constitution: &quot;All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.&quot; &quot;Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein. This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.&quot;</td>
<td>Cal. Const. art. I §§ 1, 23</td>
</tr>
<tr>
<td></td>
<td>Require government websites or state portals to establish and publish privacy policies and procedures</td>
<td>Cal. Govt. Code §11019.9</td>
</tr>
<tr>
<td></td>
<td>Permits minors to remove, or to request and obtain removal of, content or information posted on website, online service, online application, or mobile application. Prohibits operator of a website or online service directed to minors from marketing or advertising specified products or services that minors are legally prohibited from buying. Prohibits marketing or advertising products based on personal information specific to a minor or knowingly using, disclosing, compiling, or allowing a third party to do so.</td>
<td>Cal. Bus. &amp; Prof. Code §§ 22580–22582 (&quot;California’s Privacy Rights for California Minors in the Digital World Act&quot;)</td>
</tr>
<tr>
<td></td>
<td>Protects a library patron’s use records, such as written records or electronic transaction that identifies a patron’s borrowing information or use of library information resources, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries</td>
<td>Cal. Govt. Code § 6267</td>
</tr>
<tr>
<td></td>
<td>Protects information about the books Californians browse, read or purchase from electronic services and online booksellers who may have access to detailed information about readers, such as specific pages browsed. Requires a search warrant, court order, or the user’s affirmative consent before such a business can disclose the personal information of its users related to their use of a book, with specified exceptions, including an imminent danger of death or serious injury.</td>
<td>Cal. Civil Code § 1798.90 (&quot;Reader Privacy Act&quot;)</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Operator of a commercial website or online service must disclose in its privacy policy how it responds to a web browser ‘do not track’ signal or similar mechanisms providing consumers with the ability to exercise choice about online tracking of their personal information across sites or services and over time. Operator must disclose whether third parties are or may be conducting such tracking on the operator's site or service.</td>
<td>Cal. Bus. &amp; Prof. Code § 22575</td>
</tr>
<tr>
<td></td>
<td>Operator, defined as a person or entity that collects personally identifiable information from California residents through an Internet website or online service for commercial purposes, must post a conspicuous privacy policy on its website or online service (which may include mobile apps) and to comply with that policy. The privacy policy must identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its website or online service and third parties with whom the operator may share the information.</td>
<td>Calif. Bus. &amp; Prof. Code § 22575–22578 (CalOPPA)</td>
</tr>
<tr>
<td></td>
<td>Prohibits a person or entity from providing the operation of a voice recognition feature in California without prominently informing, during the initial setup or installation of a connected television, either the user or the person designated by the user to perform the initial setup or installation of the connected television. Prohibits manufacturers or third-party contractors from collecting any actual recordings of spoken word for the purpose of improving the voice recognition feature. Prohibits a person or entity from compelling a manufacturer or other entity providing the operation of voice recognition to build specific features to allow an investigative or law enforcement officer to monitor communications through that feature.</td>
<td>Cal. Bus. &amp; Prof. Code § 22948.20</td>
</tr>
<tr>
<td></td>
<td>Requires private nonprofit or for-profit postsecondary educational institutions to post a social media privacy policy on the institution's website.</td>
<td>Cal. Educ. Code § 99122</td>
</tr>
<tr>
<td></td>
<td>Requires all nonfinancial businesses to disclose to customers the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. Businesses may post a privacy statement that gives customers the opportunity to choose not to share information at no cost.</td>
<td>Cal. Civ. Code §§ 1798.83 to .84</td>
</tr>
<tr>
<td></td>
<td>Breach notification requirements when unencrypted personal information, or encrypted personal information and the security credentials, was or reasonably believed to have been acquired by an unauthorized person. Applies to agencies and businesses.</td>
<td>Cal. Civ. Code §§ 1798.29, 1798.82</td>
</tr>
<tr>
<td></td>
<td>Data security. Applies to a business that owns, licenses, or maintains personal information &amp; third-party contractors. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the information.</td>
<td>Cal Civ. Code § 1798.81.5</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>California</td>
<td>Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days, unless the data is being used as evidence in felony cases. Prohibits selling or making available ALPR data to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used. Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of &quot;personal information&quot; to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibit public agencies from selling or sharing ALPR information, except to another public agency, as specified; and require operators of ALPR systems to use that information only for authorized purposes. Establishes private right of action. Prohibits unfair competition, which includes any unlawful, unfair, or fraudulent business act or practice. Prohibits unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to a consumer. Provides a private right of action.</td>
<td></td>
</tr>
<tr>
<td>Colorado</td>
<td>Requires the state or any agency, institution, or political subdivision that operates or maintains an electronic mail communications system to adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted. The policy shall include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection under this part. Requires government websites or state portals to establish and publish privacy policies and procedures. Data security. Applies to any private entity that maintains, owns, or licenses personal identifying information in the course of the person's business or occupation. Must develop written policies for proper disposal of personal information once such information is no longer needed. Implement and maintain reasonable security practices and procedures to protect personal identifying information from unauthorized access.</td>
<td>Colo. Rev. Stat. §24–72–204.5</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Requires that video or still images obtained by “passive surveillance” by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images. Specifies that the custodian of a passive surveillance record may only access the record beyond the first anniversary after the date of creation of the record if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding. Creates exceptions allowing retention of passive surveillance records of any correctional facility, local jail, or private contract prison and passive surveillance records made or maintained as required under Federal law. Prohibits deceptive trade practices. Attorney generals and district attorneys enforce statute.</td>
<td>Col. Rev. Stat. § 24–72–113 Conn. Gen. Stat. §§ 42–110a through 42–110q</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Requires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be “publicly displayed” by posting on a web page and the policy must (1) protect the confidentiality, (2) prohibit unlawful disclosure, and (3) limit access to Social Security numbers. Employers who engage in any type of electronic monitoring must give prior written notice to all employees, informing them of the types of monitoring which may occur. If employer has reasonable grounds to believe that employees are engaged in illegal conduct and electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice. Labor Commissioner may levy civil penalties against a violator who fails to give notice of monitoring. Health data security law that applies to any health insurer, health care center or other entity licensed to do health insurance business in the state. Requires them to implement and maintain a comprehensive information security program to safeguard the personal information of insureds and enrollees that is compiled or maintained by such company. Data security law that applies to contractors, defined as an individual, business or other entity that is receiving confidential information from a state contracting agency or agent of the state pursuant to a written agreement to provide goods or services to the state. Must implement and maintain a comprehensive data-security program, including encryption of all sensitive personal data transmitted wirelessly or via a public Internet connection, or contained on portable electronic devices. Prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce. Commissioner enforces. Creates private right of action.</td>
<td>Conn. Gen. Stat. § 42–471 Conn. Gen. Stat. § 31–48d Conn. Gen. Stat. § 38a-999b Conn. Gen. Stat. § 4e-70 Conn. Gen. Stat. §§ 42–110a through 42–110q</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Delaware</td>
<td>Prohibits operators of websites, online or cloud computing services, online applications, or mobile applications directed at children from marketing or advertising on its Internet service specified products or services. When the marketing is provided by an advertising service, the operator of the service must implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business. Requires an operator of a commercial Internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet about individual users residing in Delaware to make its privacy policy conspicuously available. An operator shall be in violation of this subsection only if the operator fails to make its privacy policy conspicuously available within 30 days after being notified of noncompliance. Prohibits operators of websites, online or cloud computing services, online applications, or mobile applications from disclosing users’ personal information to law enforcement entities, governmental entities, or other persons, except under specified circumstances. Allows immediate disclosure of a user’s book service information to law enforcement entities when there is an imminent danger of death or serious physical harm. Requires a book service provider to prepare and post online an annual report on its disclosures of personal information, unless exempted from doing so. The Consumer Protection Unit of the Department of Justice has the authority to investigate and prosecute violations of the acts. Prohibits employers from monitoring or intercepting electronic mail or Internet access or usage of an employee unless the employer has first given a one-time notice to the employee. Provides exceptions for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court ordered actions. Provides for a civil penalty of $100 for each violation. Require government websites or state portals to establish and publish privacy policies and procedures. Prohibits deceptive acts in connection with the sale, lease, or advertisement of any merchandise. Gives investigative power to attorney general and creates a private right of action. Prohibits deceptive acts in connection with the sale, lease, or advertisement of any merchandise. Gives investigative power to attorney general and creates a private right of action. Prohibits operators of websites, online or cloud computing services, online applications, or mobile applications directed at children from marketing or advertising on its Internet service specified products or services. When the marketing is provided by an advertising service, the operator of the service must implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.</td>
<td>Del. Code Ann. tit. 6, § 1204C Del. Code Ann. tit. 6, § 1205C Del. Code Ann. tit. 6, § 1206C Del. Code Ann. tit. 19, § 705 Del. Code tit. 29 §9018C Del. Code Ann. tit. 6, §§ 2511 through 2527, 2580 through 2584 (“Consumer Fraud Act”) Del. Code §12B–100</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>Prohibits unfair or deceptive trade practices involving any and all parts of economic output of society.</td>
<td>D.C. Code §§ 28–3901 through 28–3913</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| **Florida** | State constitution: The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated.  
Data security law that applies to commercial entities and third-party agents (entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity). Requires reasonable measures to protect and secure data in electronic form containing personal information.  
Creates a public records exemption for certain images and data obtained through the use of an automated license plate recognition system and personal identifying information of an individual in data generated from such images. Provides that images and data containing personal information obtained from automated license plate recognition systems are confidential. Allows for disclosure to criminal justice agencies and to individuals to whom the license plate is registered in certain circumstances.  
Prohibits unfair or deceptive acts or practices in the conduct of any trade of commerce, defined as advertising, soliciting, providing, offering, or distributing commodity or thing of value. Creates private right of action. | Fla. Const. art. I §12  
| **Georgia** | License plate data may be collected and accessed only for a law enforcement purpose. The data must be destroyed no later than 30 months after it was originally collected unless the data are the subject matter of a toll violation or for law enforcement. Allows sharing of captured license plate data among law enforcement agencies. Law enforcement agencies deploying an automated license plate recognition system must maintain policies for the use and operation of the system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data.  
Broadly prohibits unfair and deceptive practices in the conduct of consumer transactions, defined as the sale, purchase, lease, or rental of goods, services, or property. Creates private right of action. | Ga. Code Ann. § 35–1–22  
| **Hawaii** | Any business or government agency that collects personal information shall provide notice upon discovery of a security breach. Establishes a council that will identify best privacy practices.  
State constitution: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right." | Haw. Stat. § 487N–1 to N–7  
Haw. Const. art. I §§ 6, 7 |
<table>
<thead>
<tr>
<th>State</th>
<th>Summary and/or Relevant Provisions</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idaho</td>
<td>Prohibits use of drones to capture images of people or gather information about individuals in the absence of a warrant or written consent.</td>
<td>Idaho Code § 21–213</td>
</tr>
<tr>
<td></td>
<td>Imposes regulations on individual student data, restricts secondary uses of such data, and provides for data destruction.</td>
<td>Idaho Code § 33–133</td>
</tr>
<tr>
<td></td>
<td>Broadly prohibits unfair or deceptive acts and practices in the conduct of any trade or commerce. An unconscionable act is a violation whether it occurs before, during, or after the transaction.</td>
<td>Idaho Code Ann. §§ 48–601 through 48–619 (&quot;Consumer Protection Act&quot;)</td>
</tr>
<tr>
<td>Illinois</td>
<td>Prohibits state agency websites to use cookies or other invasive tracking programs to monitor viewing habits.</td>
<td>Ill. Rev. Stat. ch. 5 §177/10</td>
</tr>
<tr>
<td></td>
<td>Limits on collection and storage of biometric data.</td>
<td>740 Ill. Comp. Stat. 14/1 (Biometric Information Privacy Act)</td>
</tr>
<tr>
<td></td>
<td>State constitution: &quot;The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or intercepts of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized.&quot;</td>
<td>Ill. Const. art. I, §6</td>
</tr>
<tr>
<td></td>
<td>Makes it unlawful for an employer or prospective employer to request or require an employee or applicant to authenticate or access a personal online account in the presence of the employer, to request or require that an employee or applicant invite the employer to join a certain group, or join an online account established by the employer; prohibits retaliation against an employee or applicant.</td>
<td>820 Ill. Comp. Stat. 55/10 (Right to Privacy in the Workplace Act)</td>
</tr>
<tr>
<td></td>
<td>Broadly prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.</td>
<td>815 Ill. Comp. Stat. 505/1 through 505/12</td>
</tr>
<tr>
<td>Indiana</td>
<td>Data Security. Applies to database owner, defined as a person that owns or licenses computerized data that includes personal information. Must implement and maintain reasonable procedures, including taking any appropriate corrective action for breaches.</td>
<td>Ind. Code § 24–4.9–3–3.5</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Iowa</td>
<td>Prohibits unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Creates private right of action for a person relying upon an uncured or incurable deceptive act.</td>
<td>Ind. Code §§ 24–5–0.5–1 to -12 (“Deceptive Consumer Sales Act”)</td>
</tr>
<tr>
<td>Iowa</td>
<td>Require government Websites or state portals to establish and publish privacy policies and procedures.</td>
<td>Iowa Code § 22.11</td>
</tr>
<tr>
<td>Iowa</td>
<td>Prohibits unfair and deceptive acts in connection with the lease, sale, or advertisement of any merchandise. Enforceable only by the Attorney General, unless there was intent to cause reliance upon the act in which case consumers can enforce the prohibition.</td>
<td>Iowa Code §§ 714.16 through 714.16A</td>
</tr>
<tr>
<td>Kansas</td>
<td>Defines breach of privacy such as intercepting phone calls and private messages, use of recording devices inside or outside of a place without prior consent, use of video recording without prior consent. Does not apply to utility companies where recording communications is necessary in order to provide the service/utility requested.</td>
<td>K.S. Stat § 21–6101</td>
</tr>
<tr>
<td>Kansas</td>
<td>Data security. Applies to a holder of personal information (a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person.) Must implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure.</td>
<td>K.S. § 50–6,139b</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Prohibited uses of personally identifiable student information by cloud computing service provider Department procedures and regulations, including appropriate procedures to protect against unauthorized access to or use of personal information</td>
<td>Ky. Rev. Stat. Ann. 171.450</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Prohibits unfair, deceptive, and unconscionable acts relating to trade or commerce. Private cause of action only to person who purchases or leases goods or services.</td>
<td>Ky. Rev. Stat. Ann. §§ 367.110 through 367.990 (“Consumer Protection Act”)</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Louisiana</strong></td>
<td>Data security law applies to any person that conducts business in the state or that owns or licenses computerized data that includes personal information. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Personal information includes name, SSN, driver’s license or state ID number, account numbers, passport numbers, or biometric data, but excludes information lawfully made public from federal, state, or local government records. State constitution: “Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.” Prohibits unfair or deceptive acts and practices in the conduct of any trade or commerce, including advertising. Creates private right of action.</td>
<td>La. Rev. Stat. 51:3071 to :3077 (“Database Security Breach Notification Law”) La. Const. art. I § 5 La. Rev. Stat. Ann. §§ 51:1401 to :1420</td>
</tr>
<tr>
<td><strong>Maine</strong></td>
<td>Require government websites or state portals to establish and publish privacy policies and procedures. Prohibits the use of automatic license plate recognition systems except for certain public safety purposes. Provides that data collected is confidential and may be used only for law enforcement purposes. Data collected may not be stored more than 21 days. Prohibits unfair or deceptive practice in the conduct of any trade or commerce, including advertising. Creates private right of action for any person who purchases or leases goods, services, or property as a result of an unlawful practice or act under the law.</td>
<td>1 M.R.S.A. § 542 29-A M.R.S.A. § 2117-A Me. Rev. Stat. Ann. tit. 5, §§ 205A to 214 (“Unfair Trade Practices Act”)</td>
</tr>
<tr>
<td><strong>Maryland</strong></td>
<td>Data security provisions apply to businesses and nonaffiliated third party/service provider. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. Personal information includes name, SSN, driver’s license or state ID number, account numbers, TIN, passport number, health information, biometric data, user name or e-mail address in combination with password or security question.</td>
<td>Md. Code Com Law §§ 14–3501 to –3503</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.</td>
<td>Mass. Gen. Laws Ch. 214 § 1B</td>
</tr>
<tr>
<td></td>
<td>Data security law applies to any person that owns or licenses personal information. Authorizes regulations to ensure security and confidentiality of customer information in a manner fully consistent with industry standards. The regulations shall take into account the person’s size, scope and type of business, resources available, amount of stored data, and the need for security and confidentiality of both consumer and employee information.</td>
<td>Mass. Gen. Laws Ch. 93H § 2(a)</td>
</tr>
<tr>
<td></td>
<td>Prohibits unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce. Creates private right of action.</td>
<td>Mich. Comp. Laws §§ 445.901 to .922</td>
</tr>
<tr>
<td>Minnesota</td>
<td>Requires Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Prohibit disclosure of personally identifying information, and requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.</td>
<td>Minn. Stat. §§ 325M.01 to .09</td>
</tr>
<tr>
<td></td>
<td>Require government websites or state portals to establish and publish privacy policies and procedures.</td>
<td>Minn. Stat. § 13.15</td>
</tr>
<tr>
<td></td>
<td>Makes a misdemeanor to publish or disseminate of advertisements which contain any material assertion, representation, or statement of fact which is untrue, deceptive, or misleading</td>
<td>Minn. Stat. Ann. § 325F.67</td>
</tr>
<tr>
<td></td>
<td>Prohibits act, use, or employment by any person of any fraud, false pretense, misleading statement, or deceptive practice, with the intent that others rely on it in the sale of any merchandise</td>
<td>Minn. Stat. §§ 325F.68</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Mississippi</td>
<td>Data security law that applies to any person who conducts business in the state and in the ordinary course of business. Personal information includes name, SSN, driver’s license or state ID number, or financial account numbers. Broadly prohibits unfair and deceptive practices as long as they are in or affecting commerce. Only attorney general can enforce the prohibitions.</td>
<td>Miss. Code Ann. §§ 75–24–1 to –27</td>
</tr>
<tr>
<td>Missouri</td>
<td>Defines “E-book” and “digital resource or material” and adds them to the items specified in the definition of “library material” that a library patron may use, borrow, or request. Provides that any third party contracted by a library that receives, transmits, maintains, or stores a library record may not release or disclose all or a portion of a library record to anyone except the person identified in the record or by a court order. Prohibits unfair or deceptive trade practices or omissions in connection with the sale or advertisement of merchandise in trade or commerce, whether the act was committed before, during, or after the sale, advertisement, or solicitation. Any person who purchases or leases merchandise and suffers loss as a result of the unlawful act may bring a civil action.</td>
<td>Mo. Rev. Stat. §§ 407.010 to -.307 (“Merchandising Practices Act”)</td>
</tr>
<tr>
<td>Montana</td>
<td>Require government website or state portals to establish and publish privacy policies and procedures. Allows sale and disclosure to third parties, provided notice and consent. State constitution: The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest. Prohibits methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.</td>
<td>Mont. Code Ann. §§ 2–17–550 to -553</td>
</tr>
<tr>
<td>Nebraska</td>
<td>Data security law applies to any individual or commercial entity that conducts business in Nebraska and maintains personal information about Nebraska residents. Must establish and maintain reasonable security processes and practices appropriate to the nature of the personal information maintained. Ensure that all third parties to whom the entity provides sensitive personal information establish and maintain reasonable security processes and practices appropriate to the nature of the personal information maintained. Prohibits employers from accessing an applicant or an employee’s personal Internet accounts and taking adverse action against an employee or applicant for failure to provide any information related to the account; prohibits retaliation against an employee who files a complaint under the Act; prohibits an employee from downloading or transferring any private proprietary information or financial data to a personal Internet account without authorization.</td>
<td>Neb. Rev. Stat. §§ 87–801 to -807</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Nebraska</td>
<td>Requires any governmental entity that uses an automatic license plate reader (ALPR) system to adopt a policy governing use of the system. Governmental entities also must adopt a privacy policy to ensure that captured plate data is not shared in violation of this act or any other law. The policies must be posted on the Internet or at the entity’s main office. Requires annual reports to the Nebraska Commission on Law Enforcement and Criminal Justice on ALPR practices and usage. Provides that captured plate data is not considered a public record. Broadly prohibits unfair or deceptive trade practices in the conduct of any trade or commerce. Creates private right of action.</td>
<td>Neb. Rev. Stat. §§ 60–3201 to 3209</td>
</tr>
<tr>
<td>Nevada</td>
<td>Requires operators of Internet websites or online services that collect personally identifiable information from residents of the state to notify consumers about how that information is used. Require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Data security. Applies to data collector that maintains records which contain personal information and third parties to whom they disclose. Must implement and maintain reasonable security measures Prohibits deceptive trade practices, including knowingly making any other false representation in the course of a business or occupation. Also prohibits failing to disclose material fact in connection with sale or lease of goods or services. Private right of action created under Nev. Rev. Stat. § 41.600.</td>
<td>Nev. Rev. Stat. §§ 603A.340, 603A.210, 603A.215, 598.0903 to .0999</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>Prohibits government officials from obtaining access to customer financial or credit records, or the information they contain, held by financial institutions or creditors without the customer’s authorization, an administrative subpoena, a search warrant, or a judicial subpoena Makes a crime to willfully intercept any telecommunication or oral communication without the consent of all parties to the communication. It is unlawful to willfully use an electronic, mechanical, or other device to intercept an oral communication or to disclose the contents of an intercepted communication. Law enforcement needs warrant, exception to warrant, or consent to use cell site simulators. State constitution: An individual’s right to live free from governmental intrusion in private or personal information is natural, essential, and inherent. Broadly prohibits unfair method of competition or any unfair or deceptive practice in the conduct of any trade or commerce within the state. Creates private right of action.</td>
<td>N.H. Rev. Stat. §§ 355–C:4, 570–A:2 to A:2-a, Const. Pt. 1, art. II, §§ 358–A:1 to -A:13</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New Jersey</td>
<td>Prohibits act, use, or employment by any person of any unconscionable commercial practice, deception, fraud, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with the intent that others rely upon it in connection with the sale or advertisement of any merchandise or real estate. Creates private right of action.</td>
<td>N.J. Stat. Ann. §§ 56:8–1 to -91</td>
</tr>
<tr>
<td>New Mexico</td>
<td>Data security law applies to a person that owns or licenses personal identifying information of a New Mexico resident. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure.</td>
<td>N.M. Stat. §§ 57–12C–4, to 12C–5</td>
</tr>
<tr>
<td>New Mexico</td>
<td>Prohibits unfair, unconscionable, and deceptive practices involving goods, services, credit, or debt collection, made in the course of the person’s trade or commerce. Private right of action.</td>
<td>N.M. Stat. §§ 57–12–1 to -22 (&quot;Unfair Practices Act&quot;)</td>
</tr>
<tr>
<td>New York</td>
<td>Require government Websites or state portals to establish and publish privacy policies and procedures</td>
<td>N.Y. State Tech. Law § 201 to 207</td>
</tr>
<tr>
<td>New York</td>
<td>Prohibits deceptive acts in the conduct of any business, trade, or commerce or service. Only attorney general can enforce prohibitions on repeated fraudulent acts or unconscionable contract provisions.</td>
<td>N.Y. Exec. Law §§ 6312; N.Y. Gen. Bus. Law §§ 349 and 350</td>
</tr>
<tr>
<td>North Carolina</td>
<td>Requires state or local law enforcement agencies to adopt a written policy governing the use of an ALPR system that addresses databases used to compare data obtained by the system, data retention and sharing of data with other law enforcement agencies, system operator training, supervision of system use, and data security and access. Requires audits and reports of system use and effectiveness. Limits retention of ALPR data to no more than 90 days, except in specified circumstances. Provides that data obtained by the system is confidential and not a public record. Creates private right of action.</td>
<td>N.C. Gen. Stat. §§ 20–183.30 to .32</td>
</tr>
<tr>
<td>North Dakota</td>
<td>Prohibits an act, use, or employment of any deceptive act or practice, fraud, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise. Acts or advertisements which causes or is likely to cause substantial injury to a person and not reasonably avoidable by the injured person and not outweighed by countervailing benefits to consumers or to competition, is declared to be an unlawful practice. Creates private right of action.</td>
<td>N.D. Cent. Code §§ 51–15–01 to -11</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ohio</td>
<td>Data security law that applies to Business or non-profit entity that accesses, maintains, communicates, or handles personal information or restricted information. To qualify for an affirmative defense to a cause of action alleging a failure to implement reasonable information security controls resulting in a data breach, an entity must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information. Prohibits unfair, unconscionable, or deceptive trade practices in connection with a consumer transaction, regardless of whether the act occurs before, during, or after the transaction.</td>
<td>Ohio Rev. Code Ann. §§ 1354.01 to 1354.05</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>Requires public reporting of which student data are collected by the state, mandates creation of a statewide student data security plan, and limits the data that can be collected on individual students and how that data can be shared. It establishes new limits on the transfer of student data to federal, state, or local agencies and organizations outside Oklahoma.</td>
<td>70 Okl. Stat. Ann. §§ 3–168 (Student Data Accessibility, Transparency and Accountability Act)</td>
</tr>
<tr>
<td>Oregon</td>
<td>Data security law that applies to any person that owns, maintains, or otherwise possesses data that includes a consumer’s personal information that is used in the course of the person’s business, occupation or volunteer activities. Must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the personal information, including disposal of the data. Prohibits unconscionable tactics and other unfair or deceptive conduct only after the Attorney General has first established a rule declaring that conduct to be unfair or deceptive.</td>
<td>Or. Rev. Stat §§ 646A.622 through 646A.656</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>Prohibits unfair or deceptive practices in the conduct of any trade or commerce. Creates private right of action.</td>
<td>73 Pa. Stat. Ann. §§ 201–1 through 201–9.3</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>Data security measure applies to a business that owns or licenses computerized unencrypted personal information &amp; a nonaffiliated third-party contractor. Must implement and maintain a risk-based information security program with reasonable security procedures and practices appropriate to the nature of the information. Prohibits unfair or deceptive practices in the conduct of any trade or commerce. Creates private right of action.</td>
<td>R.I. Gen. Laws §§ 6–13.1–1 through 6–13.1–27</td>
</tr>
<tr>
<td>South Carolina</td>
<td>Requires government Websites or state portals to establish and publish privacy policies and procedures.</td>
<td>S.C. Code Ann. §§ 30–2–40</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>South Dakota</td>
<td>Data security law that applies to a person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of the state. Requires a licensee to develop, implement and maintain a comprehensive information security program based on the licensee's risk assessment. Establishes requirements for the security program, such as implementing an incident response plan and other details.</td>
<td>S.C. Code § 38–99–10 to -100.</td>
</tr>
<tr>
<td></td>
<td>State constitution: The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.</td>
<td>S.C. Const. art. I, §10</td>
</tr>
<tr>
<td>Tennessee</td>
<td>Prohibits knowing and intentional deceptive acts in connection with the sale or advertisement of merchandise.</td>
<td>S.D. Codified Laws §§ 37–24–1 through 37–24–35, amended by 2019 South Dakota Laws Ch. 177 (SB 20)</td>
</tr>
<tr>
<td></td>
<td>Requires the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system to adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted. The policy shall include a statement that correspondence may be a public record under the public records law and may be subject to public inspection under this part.</td>
<td>Tenn. Code § 10–7–512</td>
</tr>
<tr>
<td></td>
<td>Provides that any captured automatic license plate data collected by a government entity may not be stored for more than 90 days unless they are part of an ongoing investigation, and in that case provides for data to be destroyed after the conclusion of the investigation.</td>
<td>Tenn. Code § 55–10–302</td>
</tr>
<tr>
<td></td>
<td>Prohibits specific unfair or deceptive acts or practices limited to those enumerated which affect the conduct of any trade or commerce. Only attorney general can bring an enforcement action.</td>
<td>Tenn. Code Ann. §§ 47–18–101 through 47–18–125</td>
</tr>
<tr>
<td>Texas</td>
<td>Data security measure that applies to a business or association that collects or maintains sensitive personal information. (Does not apply to financial institutions). Requires implementation of reasonable procedures, including taking any appropriate corrective action.</td>
<td>Tex. Bus. &amp; Com. Code §521.052</td>
</tr>
<tr>
<td></td>
<td>Prohibits false, unconscionable and deceptive acts in the conduct of any trade or commerce. Consumer protection division can enforce</td>
<td>Tex. Bus. &amp; Com. Code Ann. §§ 17.41 through 17.63</td>
</tr>
<tr>
<td>State</td>
<td>Summary and/or Relevant Provisions</td>
<td>Source</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Utah</td>
<td>Require all nonfinancial businesses to disclose to customers, in writing or by electronic mail, the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. Provides a private right of action. Requires government websites or state portals to establish privacy policies and procedures. Data security. Applies to any person who conducts business in the state and maintains personal information. Must implement and maintain reasonable procedures. Amended in 2019 to define is subject to a civil penalty. Captured license plate data are a protected record if the captured plate data are maintained by a governmental entity. Provides that captured plate data may only be shared for specified purposes, may only be preserved for a certain time, and may only be disclosed pursuant to specific circumstances such as a disclosure order or a warrant. Government entities may not use privately held captured plate data without a warrant or court order, unless the private provider retains captured plate data for 30 days or fewer. Prohibits deceptive and unconscionable acts or practices by suppliers in connection with a consumer transaction, regardless of whether it occurs before, during, or after the transaction. Private right of action.</td>
<td>Utah Code Ann. §§ 301 to 63D–203, –201, 2.2–3800</td>
</tr>
<tr>
<td>Vermont</td>
<td>Prevents employers from requesting passwords to personal Internet accounts to get or keep a job. Data security. Applies to Data brokers—businesses that knowingly collect and license the personal information of consumers with whom such businesses do not have a direct relationship. Must implement and maintain a written information security program containing administrative, technical, and physical safeguards to protect personally identifiable information. Broadly prohibits unfair or deceptive acts or practices in commerce.</td>
<td>21 V.S.A. § 495, 9 V.S.A §§ 2446–2447</td>
</tr>
<tr>
<td>Washington</td>
<td>State constitution: No person shall be disturbed in his private affairs, or his home invaded, without authority of law. Prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. Private right of action.</td>
<td>Wash. Const. art. I, § 7, Wash. Rev. Code §§ 19.86.010 through 19.86.920</td>
</tr>
<tr>
<td>West Virginia</td>
<td>Student data law governing use sharing of student privacy rights, and notification of transfer of confidential information.</td>
<td>W. Va. Code, §18–2–5h</td>
</tr>
</tbody>
</table>
The CHAIRMAN. Well, thank you very, very much.
And we will now proceed to questions. Mr. Polonetsky, let me begin with you. And I referred to this in my opening statement.

Both the GDPR and the CCPA are written to give consumers more control over their data by establishing certain rights. These rights include the right to access, right to erasure or deletion, right to data portability, and others.

I mentioned in my opening statement a concern that these rights may inadvertently decrease privacy for consumers because companies may be compelled to retain, track, or re-identify data that they would otherwise have discarded. So if you would comment about that and then I will ask the others if they have got any observations.

Mr. POLONETSKY. I think we can effectively provide people strong rights of access and deletion if we carefully make it clear that we are not going to be requiring companies to do more tracking in order to be able to provide that data. Certainly GDPR goes in that direction. I think it is solvable by making it clear that you need to know who you are providing data to. You need to clearly verify so that you are providing the data to the person and not creating an opportunity for data breaches. But I think carefully crafting the right in a way that gives us those protections is quite feasible.

The CHAIRMAN. Is that a problem that has been experienced under GDPR? I just did not understand exactly what you were saying there.

Mr. POLONETSKY. GDPR certainly makes it clear that you are not obligated to do extra tracking in order to have the data to provide back to people. I think there have been some concerns, since the CCPA is new, in exactly what it means to verify somebody is not quite clear. So people are looking for guidance. I think one of the reasons I argue this committee should act and, indeed, override CCPA is we can fix some of those areas where there is clarity so that people have a strong right of access and we do not create any over-disclosure by providing those deletion rights that we want to provide.

The CHAIRMAN. Is that a problem that has been experienced under GDPR? I just did not understand exactly what you were saying there.

Mr. POLONETSKY. GDPR certainly makes it clear that you are not obligated to do extra tracking in order to have the data to provide back to people. I think there have been some concerns, since the CCPA is new, in exactly what it means to verify somebody is not quite clear. So people are looking for guidance. I think one of the reasons I argue this committee should act and, indeed, override CCPA is we can fix some of those areas where there is clarity so that people have a strong right of access and we do not create any over-disclosure by providing those deletion rights that we want to provide.

The CHAIRMAN. OK.

Mr. Steyer.

Mr. STEYER. So thanks, Mr. Chairman. A couple of things.

One, in California a few years ago, we passed a bill called The Eraser Button, and the point was you could erase—kids under 18 could have erased any content that they had foolishly posted without thinking about it. We think that that idea is something that should also be part of a broader Federal law.

The issue has actually been the enforcement. So my colleague on my left mentioned the enforcement issues. That has been the biggest issue around the erasure issue. And actually I am sure that Ms. Dixon knows that because there is a right in Europe to be for-
57

Ms. Guliani. I mean, I think absolutely. I mean, the average consumer does not know what data is being collected on them and does not necessarily know how to make sure that that data is accurate or to request deletion. So that is something that can certainly be accomplished while accommodating, I think, the interests of not wanting to encourage businesses to retain more information.

I will note that the right to be forgotten is not something that we would want to be adopted identically in the U.S. There are potential First Amendment considerations. For example, we would not want an individual to be able to request that a newspaper published an article about them that was disparaging take down that content. So there might need to be some modifications from GDPR to be consistent with the U.S. Constitution.

The CHAIRMAN. Thank you.

Ms. Dixon, let me shift just in the few moments I have left. There is information that after the GDPR went into effect, a number of small businesses had to shut down because they simply could not afford to comply. Is that a concern, and what do you say to that? And what advice do you have for this Congress?

Ms. Dixon. I mentioned earlier, Chairman, that the tasks of data protection authorities in the EU are broad, and one of our key tasks in advance of GDPR was to prepare industry and in particular SMEs and micro-enterprises. And in doing so, we heard a lot of concerns from smaller companies about their ability to comply with what is a vast and sometimes technical and complex law.

However, through the awareness campaign that we rolled out and the very specific guidance we were able to issue to smaller enterprises, we were able to clarify the risk-based approach that the GDPR endorses, in other words, that organizations only need to implement what are called the organizational and technical measures appropriate to the levels of risk in the scale of personal data processing that they are undertaking.

So, in fact, the GDPR does consider smaller enterprises. Some very specific articles in the GDPR, like article 30, the requirement to document data processing operations—it recognizes that smaller scale enterprises do not need to conduct that particular exercise.

So I think for every organization, the GDPR is a win-win when it is implemented. It engenders the trust of consumers. It protects organizations. And we have not seen any direct evidence of organizations having to shut down because they could not meet the com-
pliance burden once they understood how they could practically implement it.

The CHAIRMAN. Thank you.

Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman.

Again, thank you, everybody, for your testimony.

Ms. Guliani, it is good to hear from you and Mr. Steyer about the California law and its need for improvements. I can guarantee you one of the first calls I made when taking over this spot was to Attorney General Becerra, a former colleague, to ask him about the California law. And he said basically what you articulated, Ms. Guliani, that it needs improvement and that he sought to seek that.

So I wondered—Ms. Guliani, you were very clear on the discriminatory practices in housing and employment, race and gender issues that are being deployed. To your point of people not even knowing how the information is used and collected, who do you think is the repository for all of these violations that are existing today? Do you think we get that from you, the AGs? Like who do you think has the running list of duplicitous actions that are being used against people with their data?

Ms. GULIANI. I do not think anybody has a running list, which is why I think it is so important that we have robust enforcement on multiple levels. So we need the FTC to be resourced and have the technical expertise. They should also be able to level civil penalties.

But at the same time, I think we want to take advantage of State attorneys general and regulatory agencies who have a long history of protecting consumers.

And finally, I think consumers have to have the right to go to court themselves. I mean, there may be many cases where either State or Federal authorities do not have the resources and so, for good reason, cannot follow up on a privacy violation.

I think without a multi-pronged approach from an enforcement standpoint what you will effectively have are gaps and gaps that can be exploited.

Senator CANTWELL. Well, I think to the issues that you mentioned, these are things that we batted down in other areas of the law. So to see them pop up online would be really just an undermining of current Federal law. So that is why it is so important that we fight against it to make sure that the online world meets the same standard as broadcasters have to meet in the broadcast world or health care officials have to meet in other forms of health care. We do not allow those things to pop up.

I think the one thing that we learned from the Facebook hearing or Facebook writ large is just that anytime you see a survey online, chances are that information is just a data collection source so that some information can be used against you. Or when you have that familiar do you want a call back from somebody on the service is really a can I sell your name to someone else who is going to then try to solicit something from you.

So I think it is very important that we get a handle on these current privacy violations so that the public has a better understanding.
To this point about the erasing of data, one thing that we have learned from our privacy law that we passed through this Committee on clearing your good name, which was a tool by which we gave those who were victims of identity theft the ability to get a claim through the FTC and basically present that to law enforcement that they were the victim, not the perpetrator of the crime. How do you see enforcement working on something like that? Because to me, it is a very big challenge to have—you know, the standard which we are operating now is basically people call attorney generals and attorney generals basically prosecute these people and get them shut down. Really, that is what happens. Consumers call in and complain.

And so in this case, there is a lot data and information being used and they do not even know how it is being used and they do not even know that they are, as you said, on housing or loans being discriminated against.

Ms. GULIANI. Yes. I mean, I think that you really touch an important point, and one is that it is hard to figure out when a privacy violation has occurred or discriminatory conduct has occurred. I mean, just think about discriminatory advertising. I do not know the ads I have not seen, and so how do I know that I have been denied the opportunity for, let us say, an employment opportunity because I am a woman or a person of color. And so I think that it is really important that, one, the standards be clear so that companies know the rules of the road and, two, that the enforcement entities need to be looking at those companies, following up on those complaints when they get phone calls, having the resources to do that.

But I think another thing that we also should look at is especially with algorithms and machine learning, more transparency, you know, companies allowing outside researchers to look at their algorithms and say, hey, this is having a disparate impact or this is having a discriminatory effect. And so we should really be encouraging those types of behaviors and encouraging companies to do risk assessments to measure potential discrimination.

Senator CANTWELL. But just to be clear, you think that these companies should face the same penalties as other companies who have violated the law that is already in existence?

Ms. GULIANI. Exactly. Self-regulation is not working and there should be robust enforcement.

Senator CANTWELL. Thank you.

The CHAIRMAN. Thank you very much.

Senator Blunt.

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

Senator BLUNT. Thank you, Chairman.

Ms. Dixon, you mentioned in your testimony that the Irish Data Protection Commission is the lead supervisory authority in the EU for a significant number of U.S. companies because of domicile and other things. I do not want you to name companies, but are there U.S. companies, 11 months now into the implementation of this, that are noncompliant with the GDPR?

Ms. DIXON. Thank you, Senator.
In the 11 months since the GDPR came into application, we have opened 17 significant investigations into potential infringement by the large U.S. tech companies. So we have reason to believe then clearly that there are potential infringements of the GDPR arising. And we are significantly advanced in a number of those investigations and intend to bring a decision and an outcome on those investigations—

Senator BLUNT. Do you have similar investigations with EU-based companies?

Ms. DIXON. We do. So overall, we have 51 significant investigations underway currently. So a subset relate to the U.S. tech companies. We supervise government and public sector also in Ireland in addition to commercial enterprises. So it is across the board.

Senator BLUNT. So it is safe to assume that in the regime that has been put in place, that U.S. companies do not have a more difficult time or an easier time, either one, than EU companies in complying?

Ms. DIXON. I think it is not a case of a more difficult or easier compliance approach. It is a risk-based approach that the GDPR endorses. And so when you have platforms that have billions of users in some cases and certainly hundreds of millions of EU persons as users, the risks are potentially higher in terms of the issues that arise around breaches and noncompliance with the principles.

Senator BLUNT. And both EU companies and U.S. companies are being fined for noncompliance?

Ms. DIXON. We will have to conclude the investigations and—

Senator BLUNT. Before the penalty?

Ms. DIXON. The investigations have not yet concluded, the first tranche that we have underway.

Senator BLUNT. All right. Thank you.

Mr. Polonetsky, Senator Schatz and I have some legislation on facial recognition, thinking that also is a significant data that uniquely recognizes people, obviously. I think we both agree that that information collected through facial recognition needs to be treated like all other personal data.

Can you share your perspective on how Congress should define personally identified information, whether that should include facial recognition and how we would treat that in a way similar or unlike other commercially collected data?

Mr. POLONETSKY. I would argue that a bill should recognize that there are special categories, sensitive categories of information, and the typical default for collecting, using, sharing that information should be a strong consent-based model. There may be places where we can see opt out or default. But certainly when it comes to sensitive data, biometric data, DNA, facial prints, fingerprints are clearly sensitive data and should be subject to a stronger consent-based standard.

Senator BLUNT. Are there best practices out there yet?

Mr. POLONETSKY. We have done a fairly detailed set of best practices as we have seen these technologies in the market. What we try to do is differentiate between facial recognition, which I think we all know, recognizing my unique ID, creating a template, and
then perhaps facial detection. How many heads are in this space? How many male or female heads? I certainly can see potential for discrimination if I treat people differently, but I do not have a unique identification. And so in our structure, we set up a tier. If a business just wants to know how many people are in the room, unique numbers of people, that might be a notice and a way to opt out, but if I am going to identify you by your name, the default ought to be that I need your permission.

Senator BLUNT. And, Mr. Steyer, I think you were at the meeting the other day the Senator and I had on the CAMRA Act.

Mr. STEYER. Right.

Senator BLUNT. Is there a facial recognition element there or concern about kids on screens?

Mr. STEYER. There should be.

And by the way, thank you very much for supporting the CAMRA Act because I think this is really an issue that is a big deal for everybody because we get it. Your personally identifiable information is really, really important.

The one thing I would say I differ with Mr. Polonetsky on is the California law basically does not differentiate between types of data. It just says all data deserve strong protection. And one thing I would urge the Committee to think about is look how California treated data. We did not actually distinguish. And Mr. Polonetsky wrote thoughtful comments for this hearing. But we think basically all data that is your personal data is really important. Obviously, stuff like facial recognition matters a lot to all of us because we understand it. We think all data matters.

Senator BLUNT. Thank you, and Senator Markey and I are working on the screen time, face time element of that particularly as it relates to kids.

Mr. STEYER. And thank you for doing that very much.

Senator BLUNT. Thank you, Chairman.

The CHAIRMAN. And thank you.

Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ, U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman.

Thank you for the testimonies. We have had a constructive conversation.

I want to start with the FTC. My view is that any law ought to have—and this is for Mr. Steyer and Ms. Guliani—first fine authority and APA rulemaking authority. And I just want to get your view on whether you agree with that? Mr. Steyer.

Mr. STEYER. I completely agree with that. I mean, if you really look at it in a practical common sense way—and Attorney General Becerra you guys were referring to who was angry at me because we passed a law—because he is my law school classmate and friend said, “Oh, my God, now I became the Chief Privacy Officer in California.”

The big issue is resources for enforcement. You could speak to Attorney General Becerra.

Senator SCHATZ. I will get to that, sir. It is a yes.

Mr. STEYER. Yes, definitely to your question.
Ms. Guliani. Yes, definitely.

Senator Schatz. And let us talk about resources for enforcement. So the Ireland DPA has 135 employees. They are about one and a half percent of the U.S. population. The FTC has, obviously, more employees, but as it relates to—full-time privacy staff has 40.

Do we need more human beings at the FTC devoted to privacy?

Mr. Steyer. Yes, absolutely. No brainer.

Ms. Guliani. Yes, absolutely and increase technical expertise. I think as you note, the size of the FTC is probably smaller than the DC office of a lot of major tech companies.

Senator Schatz. That is a fair point. OK.

Let me go back to transparency and control. I have been banging this drum for a while. I am great with transparency and control. I just do not think it is enough. And as we think about Senator Blunt and I working on facial recognition, you are going to walk into a mall and this idea that there will be sensors everywhere and they will be pinging off of your face. And then let us say we pass a pretty robust transparency and control regime. I am not sure how you can effectuate a transparency and control regime if your phone is not constantly giving you a notification and having you make individual micro-decisions about whether Banana Republic is going to send you a message or the Apple store or whatever. Or, heaven forbid, but what happens if you did not bring your phone into the mall? How do you even say no to some of this data collection?

It seems to me that we do need belt and suspenders, that we ought to be able to turn the dials on some of these decisions. But we also need to recognize the impracticability in an IoT universe of transparency and control of giving any real control. I mean, to Chairman Wicker's point in his opening statement, is that really a choice.

I am wondering, Mr. Steyer and then Ms. Guliani, how much of this do you think can be accomplished through transparency and control, and how much of this do you think ought to be backed up with a principle of, listen, we are going to configure a statute best we can, but in order to future-proof this and in order to back this thing up, we have to have a basic principle in the law which says you may not harm people with the data that you collect? Mr. Steyer.

Mr. Steyer. I completely agree with you. You could have written my remarks. I agree with you. Transparency and control are important, but they are simply not enough by themselves.

And we talked about the rights to access, to delete, to port your information. And certain acts should be completely off limits like behavioral ads targeting kids. So transparency and control are important, but they are simply not enough. Notice and consent, sort of broad terms like that, just are not enough. We have to go farther. And we think that the public would love you to do that.


Ms. Guliani. I think you are absolutely right. Notice and consent is not enough in part because in a lot cases people do not have meaningful choices. If the option is between not having a service at all or turning over massive amounts of data, a lot of consumers consent, but it is not really consent. So I think that the law should place strict guardrails on what companies can and cannot do. For
example, if I have a flashlight app, is it really reasonable for that app to require me to turn over all of my location data or my financial data just as a condition of using that app? I would say no.

And in the face recognition context, you know, if I want to go to the grocery store to buy food, is it really reasonable that the only option I have is a sign that notifies me that face recognition technology is being used? I do not think that that is really the control and the right that consumers want. And so absolutely we have to go beyond notice and consent to get at sort of terms that really take advantage of people's privacy and exploit their lack of choice.

Senator SCHATZ. My final question—and this will be for the record and for the entire panel—is whether or not we are missing anything in terms of essential elements of a Federal data privacy law? And I will take that for the record. Thank you.

The CHAIRMAN. That is a very good question, and so I hope all of our panelists will take that for the record and you have a few days to respond. That would be very helpful.

Senator Fischer.

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

Senator FISCHER. Thank you, Mr. Chairman.

One core part of the GDPR is to protect consumer data by requiring freely given, specific and informed consent. However, we already are seeing user interface workarounds that we can consent by confusing user choice. Ms. Guliani, you just spoke to that in the answer to Senator Schatz's question.

In these circumstances, users see a false choice or a simple escape route through the “I agree” button or “okay” button that pops up on our screen. And this can hide what the action actually does, such as accessing your contacts, your messages, Web activity, or location. Users searching for the privacy friendly option, if it exists there at all, often must click through a much longer process and many screens.

Mr. Steyer, is clear, easy to understand user interface design a critical component of achieving informed consent and preserving any rights to consumer data privacy?

Mr. STEYER. That is a great question, Senator Fischer, and it is. It really is. I think the truth is if we all think about ourselves—maybe there are one or two wizards up here, but I am not and I run a large organization that helps write privacy laws.

So I think clear, easy-to-use information is absolutely critical. That is why I mentioned it in my opening remarks. This is complex stuff, and so we need to make it very easy for consumers to understand what their rights are and then how to exercise them. It is like having a privacy policy at the end of your phone, 80 pages on your phone, which no one ever reads. They just check here. So I think that is a really important element of what this committee and the Senate could do is make it simple and easy to understand for the consumer. If it is easy to understand for you folks, it will be fair to the consumer would be what I would say.

Senator FISCHER. I hope that is an endorsement.

[Laughter.]
Mr. Steyer. That is an endorsement, but it is also recognizing the complexity of this. It actually goes to the question Senator Schatz was asking. But it is really an important element of doing this right.

Senator Fischer. Right.

I appreciated Common Sense Media’s endorsement of the bill that I have with Senator Warner, the DETOUR Act, and I believe that is going to guard against the manipulative user interfaces that are out there. Those are also known as dark patterns.

Can a privacy framework that involves consent function properly if it does not also ensure that user interface design presents that fair and transparent options to manage our personal data setting, sir?

Mr. Steyer. Is that directed to me?

Senator Fischer. Yes, please.

Mr. Steyer. You are absolutely right on that.

By the way, the other point I would make is the fact that you and Senator Warner are working on the dark patterns, the fact that Senator Blunt is working with Senator Markey and others on bipartisan legislation, this is an area where—I keep saying it. This is common sense for everybody, and I really do believe that this committee, acting this way in a bipartisan fashion, is critical.

But, yes, we have got to keep it simple and easy. Even though it is complex, you have got to make it simple and easy for the average user.

Senator Fischer. Thank you.

Ms. Dixon, as the GDPR has been implemented, have you seen any trends for companies that have taken steps toward focusing on user-centered design or others that are avoiding it on purpose?

Ms. Dixon. We certainly, in the run-up to the GDPR, saw a lot of attempts in particular by the platforms to redesign their user engagement flow and to reexamine whether the consents they were collecting met the threshold articulated in the GDPR. But some of the investigations that we now have underway are looking at whether the ways in which in particular the transparent information is being delivered to users really meets the standards anticipated by the GDPR.

So, for example, a lot of organizations have implemented layered privacy notices, which is something generally that we recommend to avoid the need to have a 100-page privacy notice. But on the other hand, there can be issues of inconsistency between the layers, too many layers for a user to go through to get basic information.

So through the investigations that we have ongoing at the moment, we are examining whether the standards anticipated by the GDPR are being met and in what circumstances we say they are not being met. So there should be further clarification on that in the coming months.

Senator Fischer. So as Mr. Steyer was saying, keep it simple.

Ms. Dixon. Keeping it simple is always good.

Senator Fischer. As we look to draft Federal data privacy policy, it is important that we do look at preventing irresponsible data use from the start. Ms. Dixon, you actually noted the complaint of someone who had been contacted by a headstone company after a family member passed away, generated by combining obituary data
and public address data. And I am going to ask all of you the same question that I asked the previous industry panel, and hopefully you can respond in writing to the question since I am out of time.

But I would just really appreciate if you could give one example of an unreasonable data practice to us. I think that would be helpful when we do look at trying to keep this simple and what is going to be needed. So thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Can each of you do that for us on the record? We would appreciate it if you would.

Senator Tester.

STATEMENT OF HON. JON TESTER, U.S. SENATOR FROM MONTANA

Senator Tester. Thank you, Mr. Chairman.

Thank you all for being here. I know you all came to talk about production ag today, so I am going to ask some questions about it.

I have been farming for about the last 40 years, and one of the big advances in agriculture that has happened pretty recently is called precision ag where you get computers on your tractor that measure just about everything you do, from the amount of fertilizer you put down to the kind of seeds you put in the ground, to the number of acres you cover. You name it.

So I have got this information. It is obviously connected up with a higher God. Is it possible for folks or do you know if they can use that information right now, if they can gather that information to try to influence my buying decisions? Do you understand what I am saying? I am saying we have got technology on the tractor that measures just about everything you do. Is that information gatherable? Just somebody taking that information and sweeping it up. Is it possible for them to do it? Can anybody answer that?

Ms. GULIANI. So I cannot answer specifically. I think with agriculture and some of, I think, the new technologies, I do think that a big problem is secondary uses. Right? Think about if I buy eggs from a grocery store and I give somebody my address to deliver those eggs, I expect that they are going to use my address to get the eggs to me. What I do not expect is that they are going to tell an insurance company that I bought eggs and they should charge me a higher rate.

Senator Tester. OK. So what gives them the right to do that? What gives them the right to share that information? It looks to me like why should it not all be off the books unless I say, you know, what, go ahead and give it to my doc, give it to my insurance company, give it to a guy I am going to buy a car from, I do not care, go ahead and do it. Otherwise, if I do not do that, no sharing information. Period. What I do is my business and nobody can share it. It is against the law.

Ms. GULIANI. I mean, I would agree. And I think that what functionally happens sometimes is that there is a 30-page privacy policy. Somebody does not understand what is in it, nor do they have the time to read it.

Senator Tester. So it looks to me like it does not have to be 30 pages. Does it? Could it not be just a simple question: Can we use your information, yes or no?
Ms. GULIANI. Yes. And I do not believe that there should be secondary uses and secondary sharing unless the person knows what is happening and has provided specific consent for it.

Senator TESTER. OK. So the lady from Dublin, would the GDPR stop the collection that I just talked about? And by the way, that is a scenario I use for agriculture, but you could use it on anything. Would they stop it? Would your rules stop it?

Ms. DIXON. Thank you, Senator. It is a very interesting question.

As I mentioned in my written statement, the GDPR is high-level, principles-based, technology-neutral, and it does not prohibit any specific forms of personal data processing. It provides that any form of personal data processing could be legitimized.

So in this case, what we would have to do is trace through the various actions of the company and look at whether the principles of the GDPR are being met, in particular in this case around purpose limitation, transparency to you as a user in terms of sharing the data with third parties and the purposes for which it would be used. And to the extent that consent is legitimizing the processing, whether you had granular options to consent or not to consent. And so it is possible that the GDPR would prohibit it depending on how it is being done, but it would involve the specific parsing against the principles.

Senator TESTER. A previous question asked you about fines, and you said none have been levied yet because your investigations have not been done. You have been in effect for 11 months since it was put into effect?

Ms. DIXON. It is 11 months since the GDPR came into application. Some of the investigations have been open more recently, but we have one or two that are open since May.

Senator TESTER. Since May. So we are coming on a year for the investigations?

Ms. DIXON. That is right.

Senator TESTER. How quickly are they to a point where you can—are these investigations so complicated that we are looking at another year or is it weeks?

Ms. DIXON. No. I think in the coming months over the summer, we will conclude decisions on some of them. They are complex investigations. There are also significant procedural safeguards that we have to apply because the sanctions are significant. So we do have to allow the party's right to be heard at various junctures in the investigation and decisionmaking.

In addition, because of the form of a one stop shop we have in the EU, other procedural issues arise.

Senator TESTER. And very quickly because my time has run out. How are the fines levied? How do you determine the fine? Is that dictated in the GDPR or do you do it on the size of the company?

Ms. DIXON. So article 83 of the GDPR sets out the limits on the fines and provides details of aggravating and——

Senator TESTER. Can you give me an idea of what the largest fines are under the GDPR?

Ms. DIXON. The largest fine would be 4 percent of the global turnover for the preceding year of an undertaking.

Senator TESTER. Thank you.

The CHAIRMAN. Thank you, Senator Tester.
Senator Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE

Senator Blackburn. Thank you, Mr. Chairman. And thank you to each of you for being here today. And, Mr. Steyer, good to see you.

Mr. Steyer. Nice to see you.

Senator Blackburn. We have been talking privacy for quite a while.

Mr. Steyer. We have.

Senator Blackburn. Ms. Guliani, I am certain you know this, and to our friends who have joined us today, I think that for so long what we heard on Capitol Hill from people is do not do anything that is going to harm the golden goose. Leave it alone. And this is why I introduced the BROWSER Act several years ago, bipartisan in the House, and why I have long held that consumers need to possess the toolbox to protect, as I term it, their virtual you, which is you and your presence online. And this is vitally important as Americans move more of their transactional life online.

And, Ms. Guliani, you said it well. There should not be a secondary use for other companies to know what credit cards we use, what time of month we pay our bills, the sites we search, the products we order. And for that to be data-mined and then repackaged and sold specific not to our name or physical address maybe, but to our IP address, which is our virtual you.

So that is why the BROWSER does a few things very well. It says opt in for sensitive data, opt out for non-sensitive data, and one set of rules for the entire Internet ecosystem with one regulator.

And I think when we look at an individual's privacy, that we ought to focus on doing a few things well, to do it understandably, and as we have discussed in the past, Mr. Steyer, to make certain that the protections are there for children and that their information is protected online.

And I am delighted that the chairman is bringing this issue forward. Privacy and data security are essential because this transactional life that we live online underpins every single industrial sector of our nation's economy.

And, Ms. Dixon, I want to ask you about the difference, let us say, for Ireland with having an EU-wide regime on privacy as opposed to an Ireland-specific. Preemption I think is vitally important, and I would like to hear from you what the difference has been by having the ability to have it EU-wide versus just for Ireland.

Ms. Dixon. So, Senator Blackburn, the GDPR, as you note, is a direct effect regulation of the EU as opposed to a directive which requires transposition into member state law, which was the previous regime we had prior to last May. But, in fact, as a regulation, the GDPR is still something of a hybrid because each EU member state, nonetheless, had to implement a national law to give further effect to the GDPR.

Senator Blackburn. It underpins.
Ms. Dixon. It underpins and gives further effect to the GDPR and implements some choices that were left to each individual member state under the GDPR.

So what we have is actually a hybrid where we have a 2018 Irish Data Protection Act that guides us in terms of the operation of our investigations and the procedures we must follow and around aspects such as the age of digital consent for children, which is set at 16 in Ireland, and then we have the GDPR. In the case of any conflict, which there should not be, the GDPR reigns supreme under the doctrine of supremacy of the EU law. So it is something of a hybrid, and there are still member state flavors in terms of choices made under the GDPR.

Senator Blackburn. Thank you. I appreciated a visit with your EU Privacy Commissioner a few weeks ago and then this week visited with the Commissioner from New Zealand. And I think it is instructive to us that whether it is GDPR, as it comes through its first year of enactment, or other countries that are looking at enacting privacy policy, that it is important to our citizens that we do something and that we do it right the first time. So I appreciate your participation and look forward to continuing the conversation. I yield back my time.

The Chairman. Ms. Dixon, the GDPR directs European member states to make certain decisions, for example, the age of consent. Is that what you are saying?

Ms. Dixon. So under certain articles of the GDPR, such as article 8, the age of consent for children accessing information, society services was set at 16, but it gave member states the choice to implement as low as 13 under their member state laws. So, in fact, what you find is that the majority of EU member states went ahead and implemented an age of 13. So there are a number of articles like that where member state choice was implementable.

The Chairman. Maybe we could search that ourselves. But if you would help us by supplementing your testimony and giving us some examples of that, I would appreciate it. Thank you.

Senator Peters.

STATEMENT OF HON. GARY PETERS, U.S. SENATOR FROM MICHIGAN

Senator Peters. Thank you, Mr. Chairman.

And thank you to each of our witnesses. It has been really a fascinating discussion.

And, Mr. Steyer, I do believe you are right that this is an important issue that the time is now. In fact, I think the issue of privacy, given the explosion of data and technologies with the power to collect a lot of data are continuing to expand. This could be one of the defining issues of this decade as to how we deal with it because with data comes power, and that power is based on data collected from us each individually. So we have to be leaning into this very heavily. So I agree with that.

My first question, though, for you, Ms. Guliani, is an example of some concerns that I have. There is a popular pregnancy tracking app Ovia that tracks medications, mood, bodily functions, and more and even use it to track newborn medical information for women that use this app. You may be familiar with it. The app has come
under scrutiny because it allows employers to actually pay to gain access to the details about their workers' personal lives. Your testimony—you were very clear and others have mentioned about how Federal law should limit purposes for which consumer data can be used.

So my question, though, is what should be included in a Federal privacy standard to ensure that employers, in particular, cannot have access to their employees' medical information from an app such as Ovia?

Ms. Guliani. I mean, I would say first that that is information that should not be given to an employer absent the consent of the individual using the app, and they should not be denied using it if they say, look, I do not want my employer to know that but I would still like you to measure these things. So I think that those are sort of two sides of the same coin.

And what I worry with apps like these is, again, these long privacy policies that individuals do not have time to read or understand that effectively require them to sign away all these rights just to use a service.

Senator Peters. Well, to follow up on that comment, in Ovia they have a 6,000-word consent form. The company is granted, quote, a royalty-free, perpetual, and irrevocable license throughout the universe to utilize and exploit their de-identified personal information. The company is allowed to sell, lease, or lend aggregated personal information to third parties. This basically means that all of the information that was gathered—a package can be sold to whoever they want whenever as long is it does not meet their de-identified criteria.

But how difficult is it for a company to re-identify somebody if there is enough data about them? Let us say a smaller company that may only have one woman who is pregnant—could you identify that person probably even with de-identified data?

Ms. Guliani. Yes. I mean, re-identification I think is becoming easier, and there are companies that are innovating around that. So, for example, there have been MIT studies that found that de-identified data could be re-identified 95 percent of the time with accuracy. So I think it is really important that when we talk about de-identified data, we are really clear on what that means and making sure that it is, in fact, de-identified.

Senator Peters. Right.

Mr. Polonetsky, an example. If I go to the doctor and I get prescribed an allergy medicine and then I put that information on an app that I have to keep track of the number of doses I have to take of medicine or whatever it may be, how do you envision a Federal privacy law, working with existing laws such as HIPAA, to ensure that my medical information is indeed protected after I put it on my own app?

Mr. Polonetsky. Yes. This is increasingly going to be an important issue because patients are increasingly downloading their medical records, and there is obviously great value in people being able to see that data, maybe take it to a different doctor, analyze it themselves. But they may not appreciate that once they have downloaded it from their HIPAA-covered entity, that is is now in their hands, it is in their app.
Legislation should recognize that there are sensitive categories of data that are going to be subject to much stricter and tougher controls. I may want to share that with another doctor. I may want to show it to my spouse. And so I certainly should be able to share it, but it ought to be very clear and very practical, and I ought to be able to revoke that consent.

It is not likely to be covered by HIPAA, but we increasingly have data that is outside of the regulatory world where we need to make sure that the consent standard in any proposed legislation is indeed balanced.

Senator Peters. In March, it was reported that a data broker tried to sell the names, addresses, high schools, and hobbies of 1.2 million children. This was uncovered through the violation of Vermont’s recently enacted law to regulate data brokers.

Mr. Polonetsky, as you know, the Vermont law requires data brokers to register with the state annually and gives us some transparency as to who is actually out there, who is actually collecting all this information.

Understanding that the law was just recently implemented, do you have an early assessment of the law, and should we look at that law in guiding some of our work at the Federal level?

Mr. Polonetsky. I do not have enough information to know how it is playing out, but it is clear that people today have a limited idea of the number of places their data goes when they are online or when they can transact. And providing a simpler way for them to get to those endpoints so they do not have to go to multiple places so they can say no once or they can go to one place and effectively take their data out I think is valuable.

Frankly, I think it is valuable for companies too, the people who really do not want to be getting catalogs in the mail or do not want to be marketed to. It is costly to send some of that out, and I would like to believe that at the end of the day, there is a win-win by giving people more control over what they receive from a whole range of third parties.

Senator Peters. Thank you. Appreciate it.

The Chairman. I think there are a lot of win-wins out there.

Senator Thune.

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

Senator Thune. Thank you, Mr. Chairman.

Ms. Dixon, in your testimony you touch on industry codes of conduct. Can you elaborate on how industry codes of conduct are intended to operate under the GDPR and whether you think such codes of conduct enhance compliance with the law?

Ms. Dixon. So codes of conduct are a new feature of EU data protection law, and we do believe that they are going to pay dividends once they get off the ground. The European Data Protection Board has recently issued guidance on how it is intended that codes of conduct would work. And in the first instance, it is up to industry groupings to bring forward proposed codes of conduct that they would agree to implement. They have the benefits of creating a
level playing field within industry sectors and driving up standards.

Another key feature of codes of conduct under the GDPR is that it is intended that there would be an independent monitoring body paid for by the industry sector that would monitor compliance with the code of conduct and ensure that complaints from individuals—that the exercise of their rights, for example, is not being adhered to—are dealt with efficiently. So this is an area of the GDPR that we look forward to rolling out over the coming years.

Senator Thune. Let me just direct this to everybody, and it is more of a general question. But Mr. Polonetsky, Mr. Steyer, and Ms. Guliani, with respect to privacy expectations of our consumers here in the United States, do you think the status quo is working? Yes or no?

Mr. Steyer. No, but I would tell you that there has been a sea change in awareness in the last year. I think one of the most encouraging things that we have seen, other than the bipartisanship, I think, in understanding these very issues that affect everybody, is that the public is finally coming to understand that privacy really matters. Remember, it is a fundamental right, but people have forgotten that. I have four kids, and I remember talking to my kids about this a few years ago, about do you even understand what privacy is.

So I think we are at a watersheds moment, which I think the work of this Committee and the broader Senate and Congress will drive forward. The public is finally understanding this is really my own personal information. It is really important, and I have the right to control it. So I think we are at a great moment, and I think that honestly, Senator Thune, if this Committee moves forward and the Senate moves forward, I think it will be incredibly important not just legally and from an enforcement and accountability standard for behavior, but public awareness. So I think we are at a really important tipping point that you all can drive forward in a very important way.

Mr. Polonetsky. Senator, my 17-year-old son is sitting behind me and I have got a 15-year-old daughter, and it has been fascinating to see how they have been using technology and I do not think they think about it in terms of privacy. All they know is that their Instagram page should not have all of their photos. It should have the ones they curate. And they have another account they use a little more flexibility, a little more sloppily.

My son is a big Snapchat user, and he is not thinking about it, oh, my pictures disappear. I am just saying hi. Why should that be around forever?

And so I am optimistic that the technology is finally capturing the actual reality of how people act. Somehow when some of these sites launched, the notion was the more you share, the more people click on it, the more people see your stuff. And there is a place for that, for activism, for outreach. But that is not the default for the way most of us live. We want to talk to friends and family and small groups and alumni groups and the like. And somehow the engineering answer was, sorry, if it is on the Internet and it is public, it is public for everybody.
So these are not perfect. You know, it is not perfect privacy when your photo disappears. It is probably somewhere. But it gave me a level of obscurity that actually ends up being critical and nuanced.

So I would like to see us nudge companies to solve some of these problems by having technology reflect the way humans act. Right? It is supposed to be in service of our needs, not in service solely of advertising and marketing. I see that pushback happening. I would like to think it is because of privacy pressure, but I actually think it is because of what the younger generation actually wants. And they do not call it privacy. They call it this is the way I think about my relationships.

Senator Thune. But the answer is no, the status quo is not working.

Mr. Polonetsky. The status quo is not working.

Senator Thune. Ms. Guliani, yes or no. I have another question I need to ask here.

Ms. Guliani. Yes. The status quo is not working, and I just want to highlight that I think we are increasingly understanding that that status quo is hurting vulnerable populations in some cases the most, you know, exacerbating economic inequality and some of those issues. And so I think the law should reflect the special harm that is being placed on consumers.

Senator Thune. And I agree the status quo is not working, which is exactly why this committee began to lay the groundwork for privacy legislation in the last Congress and we are building on that. I believe it is one of the issues that Congress should be able to work on together on a bipartisan basis, and I look forward to working with Chairman Wicker and other members of this Committee to find consensus on this very important issue.

One very quick final question, and that, again, I think can be yes or no. But on principle, would any of you oppose any Federal law with preemption in it? Yes or no.

Ms. Guliani. We would have serious concerns with broad Federal preemption.

Mr. Steyer. I have serious concerns with broad Federal preemption.

Mr. Polonetsky. I think preemption can be done carefully so that it preempts the inconsistencies that make compliance hard but preserve the rights and protections that I think we want to preserve.

Senator Thune. I would be interested—and I guess we can take this for the record, Mr. Chairman—in your thoughts. You all referred to a Federal law as strong as California and just to maybe speak specifically to what you mean by that.

Thank you.

The Chairman. Thank you.

And, Senator Thune, you questioned long enough for Senator Markey to get back in his seat. So Senator Markey is next.

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

Senator Markey. Thank you, Mr. Chairman, very much. And thank you, Senator Thune.
I have long advocated for privacy protections that include the principles of notice and consent, but a Federal privacy bill must build on that framework by explicitly prohibiting certain types of data use. Today companies amass troves of consumers’ data and then repurpose that information to target ads in discriminatory ways.

And that is why I recently introduced the Privacy Bill of Rights Act, comprehensive privacy legislation that bans discriminatory uses of consumers’ private information. This legislation explicitly prohibits companies from using Americans’ data to target employment, housing, health care, education, or financial opportunities in harmful, discriminatory ways.

Ms. Guliani, can you provide one example of how a company currently uses consumers’ personal data to target individuals of particular genders or socioeconomic groups in ways that threaten Americans’ civil rights?

Ms. GULIANI. Sure. I mean, I can give you a recent settlement in an ACLU case. You know, over the last several years, there were multiple charges that Facebook was facilitating discriminatory advertising, particularly in the housing, credit, and employment contexts where Federal law prohibits discrimination. So, for example, allowing targeting of ads based on factors like race or gender or things that would be proxies for that.

Over the years, complaints were made. The company said that they were going to resolve the problem but were slow to do so. And so the ACLU and other civil rights organizations filed a lawsuit, and the company, to its credit, has settled that lawsuit.

But I think what this does is speak to a broader concern, and that is a question of how in this new online ecosystem are advertisers and others exacerbating discrimination, charging different prices for, let us say, a bus ticket, not allowing African Americans or women to see employment or housing opportunities.

Senator MARKEY. So let me just follow up on that. Do each of the rest of you agree with Ms. Guliani that it should be illegal for companies to use consumers’ personal data in these harmful discriminatory ways? Ms. Dixon.

Ms. DIXON. So, Senator Markey, I think in terms of legislation prohibiting certain uses, as I have outlined, the GDPR is set up as principles-based and does not specifically prohibit uses but principles of fair processing, as an example, will go some way to tackling the issues that you have outlined.

In general, discrimination—and there is some complexity to the issue——

Senator MARKEY. But in general, do you agree with Ms. Guliani? In general on discrimination?

Ms. DIXON. In general, yes.

Senator MARKEY. OK.

Mr. Polonetsky.

Mr. POLONETSKY. In general, yes.

Senator MARKEY. Mr. Steyer.

Mr. STEYER. Absolutely I agree.

Senator MARKEY. Thank you all.

So let us move to children’s privacy. I will go to you, Mr. Steyer. Children are a unique, vulnerable group online. That is why earlier
this Congress I introduced bipartisan legislation with Senator Hawley to protect kids’ and teens’ privacy. This legislation is an update to the Children’s Online Privacy Protection Act, a law which I authored back in 1997.

This law creates critical new safeguards for young people. The legislation would extend protections to 13, 14, and 15-year-olds by requiring consent before collecting personal information about them, ban targeted ads to children, create an eraser button for parents and children to allow them to eliminate publicly available personal information submitted by the child or teen, and establish a youth privacy and marketing division at the Federal Trade Commission, which will be responsible specifically for addressing the privacy of children and minors in our country and marketing directly at children and minors in our country. We know we have a crisis in the country in terms of the targeting of children in our country by these online companies.

So, Mr. Steyer, why is it critical that any comprehensive privacy law include these heightened protections for children and teens?

Mr. STEYER. We totally support the law, and we are glad it is bipartisan. We just believe you should fold the COPPA 2.0 law into this broader law that you are doing.

The truth is—we all know this as parents and grandparents—kids do not understand stuff. They may be more technically literate in a way, but they just do not understand it. So they deserve special protections, and the COPPA 2.0 law that you all have introduced is absolutely spot on, and I would urge everybody on this committee and all 100 Senators to support it.

Senator MARKEY. Do you each agree that special protections have to be built in for children? Ms. Guliani.

Ms. GULIANI. Yes.

Senator MARKEY. Mr. Polonetsky.

Mr. POLONETSKY. Yes.

Senator MARKEY. Ms. Dixon.

Ms. DIXON. Yes.

Senator MARKEY. Mr. Steyer. Correct.

And teens. COPPA stops at 12, and we all know what teenagers are like. They need special protections too.

Senator MARKEY. So this bill would lift it up to 16.

Mr. STEYER. Correct.

And that is kind of, I think, a reasonable place to put it. I wish I could make it higher, but I think at least at 16, kids are just unaware even though you are saying technically sophisticated, but their judgment in terms of what it might mean for themselves in the long run just has not been well thought out.

Mr. STEYER. And California goes to 16. We took it up to 16 in the CCPA.

Senator MARKEY. And in Europe?

Ms. DIXON. 16 in Ireland, 13 in other member states.

Senator MARKEY. Yes. I am Irish.

[Laughter.]

Senator MARKEY. We like our privacy.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

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

Senator MORAN. Chairman, thank you.

Thank you for joining us today on this important topic.

Let me start with Mr. Polonetsky. The terms of a Federal consumer privacy bill. Consumers I believe would benefit if Congress provides clear and measurable requirements in a statutory text while also including a level of flexibility in the form of narrow and specific rulemaking authorities presumably to the FTC. That would help account for evolving technological developments.

My questions are how should this committee approach providing the FTC with rulemaking authority, and do you see value in what some of us have been calling strong guardrails around that rulemaking authority to preserve certainty to consumers that we aim to protect?

Mr. POLONETSKY. I think our proposed legislation—the Committee's proposed legislation, which hopefully will come forward should put as much detail as we can put in the bill because I think there are going to be key issues to negotiate. But clearly there are going to be areas that are going to need more time, where progress of time is going to require perhaps updates and nuance, and the FTC certainly needs APA rulemaking authority to fill those gaps. But I do think setting the parameters so that the considerations that the FTC should look at can be spelled out so that businesses can anticipate so that commission heads, no matter what party is in leading and so forth, in the right direction I think is going to be critical.

Senator MORAN. This is not exactly the right words I do not think, but the theory that I have is that we have to provide lots of certainty but not too much certainty. Where do we find that sweet spot that allows this to work well today and into the future?

Ms. Dixon, you indicated in your testimony—I think I am quoting this about right—the aim equally of a consistent and harmonized data protection law across the EU is to ensure a level playing field for all businesses and a consistent digital market in which consumers can have trust.

Would you be concerned that EU consumers' trust in the digital market would be undermined if the EU lacked a harmonized approach to privacy? And related to that is, do you think the GDPR has provided clearer privacy requirements to companies than if each EU country adopted a different privacy requirement?

Ms. DIXON. So I think certainly it would be the case that EU service users' trust would be undermined if we do not give full effect to this harmonized regulation now in the EU, and it's more a case of companies, rather than consumers, at the moment arguing that some of the harmonization is not coming into effect as anticipated because of member state choices that have been made. So the European Data Protection Board is a grouping of all of the EU national supervisory authorities, and we are working very hard to give effect to a harmonized implementation through guidance that we issue, but also through cooperation and consistency mechanisms that mean, when I conclude the investigations I referenced earlier, I will have to bring my decision to the European Data Protection Board and take utmost account of the views of the other EU 27 in finalizing my decision. So I think the harmonization is extremely
important not just in terms of a level playing field, but in terms of the consumer trust.

Senator Moran. Thank you.

Part of the conversation here has been things are getting better. People are more interested in privacy. But we have also talked about how difficult it is to—what you are thinking about when you opt in and opt out, where the responsibility lies.

Are consumers currently considering privacy practices when choosing between an online service provider? Are there enough companies using privacy as a competitive advantage? Any consumer paying attention to this and there is now an economic reward for privacy protections?

Mr. Steyer. I would like to speak to that. I think when we passed the California bill last year, we were working with Satya Nadella at Microsoft, Tim Cook at Apple, Mark Benioff at Salesforce. They absolutely know that—there is no way that Apple and Microsoft do not see that as a competitive advantage now which, Senator Moran, I think is a very healthy thing.

But that alone is not enough. That is why I said in my earlier comments about how important it is for the Senate and for the Congress to pass comprehensive, strong Federal privacy protections.

But there is no question. Just look at Apple’s marketing campaign that is out there right now. They are all over privacy. We meet with them at the top levels all the time. They have decided this is both the right thing to do and also the right thing to do for their business. And so has Microsoft. So the wave is coming.

Senator Moran. What a great blend that will be if we do our jobs correctly and the consumer demands this from their providers.

Mr. Steyer. Agreed.

Senator Moran. Let me ask a final question. Just a yes or no answer. If Congress were to enact what we hope is meaningful privacy legislation, would you each support the attorney general of our various states having enforcement capabilities?

Ms. Guliani. Yes. I would strongly encourage that, as well as State enforcement agencies.

Mr. Steyer. Completely agree. Absolutely I think State AGs are critical, and a private right of action is a good idea too.

Mr. Polonetsky. AGs have a key role.

Senator Moran. Thank you all very much.

Thank you, Mr. Chairman.

The Chairman. Thank you.

Senator Rosen.

STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM NEVADA

Senator Rosen. Thank you.

This is an amazing hearing and I have so many questions.

I am going to first start with some vulnerable population questions. One of our most vulnerable populations are seniors, our disabled veterans, our hearing, our deaf community. I have over 38,000 deaf and hard of hearing people in the state of Nevada. They rely on IP captioned telephone service to communicate. We all know what that is. As privacy concerns, what are we doing to pro-
tect those vulnerable populations who are using the telephone, using these other services because of a disability?

Ms. Guliani. So I think that this is one of the reasons that having a privacy framework is so important. I mean, you mentioned the disabled population. Low income individuals rely on their phones more for Internet access and to do other day-to-day activities. And what we do not want is a system where as a condition of using these things that are critical to everyday living, people have to hand over their personal data and that personal data can have downstream consequences.

And so I think that as part of any framework, we have to consider, number one, limiting the extent to which somebody can require you to give consent just as a condition of using a service. And we also have to be really skeptical and outlaw sort of what has been called pay for privacy schemes where I am just going to charge you more if you choose to exert your privacy rights.

Mr. Polonetsky. Senator, I would urge the Committee to hear from the disability community because I think there is actually a really nuanced set of views. Certainly the community—and I will not speak for them although we have done some joint work recently—is worried about new ways that they can be discriminated against, but they are also passionate about the ways assisted technology and data—they want a smart home speaker to be able to control devices if they cannot use the traditional UI. They do not want their data sold, but getting that balance right so the data they do want can support them is certainly important.

Senator Rosen. So as I have been sitting here listening—and I get the pleasure of being one of the last questioners—is that it seems to me that there are two issues about your data. It is kind of the who, what, where, when, and how. The who is your personal data. It is your name, your birth date, your Social Security number, whatever. You own that. Right? Your baseline definition. Then you have your recorded behavior, if you will, your usage, your active usage, your passive usage. What is caught on recording and geolocation, that is your what, when, and how.

So the real issue is who owns your behavior. Right? I mean, there are new safety issues, security for your personal birthday and all those kinds of things. So who owns your behavior is the issue, and what do they do with it? And the real value and the real threat is the monetization of your usage data. That is where it is. It is economics. Let us just put it right there.

So how do you think that we can tailor some legislation that protects your usage information? We are trying to get better about protecting that personal identify, the who, but what about the what, where, when, and how that happens outside of you, where you shop, where you drive by, where you record on your voicemail?

Mr. Steyer. So, Senator Rosen, I mean, it is a very important question. It is a very good question. I think the truth is we should broadly protect—allow the individual to control not just their own data but their behavior. I used the term earlier, “data minimization.” It was one of the big issues in the California law and in GDPR, and it is a company should only be able to use the data for a necessary business purpose, not a secondary purpose. When Sen-
ator Tester was asking the question about the farm implements, why should that be sold——

Senator Rosen. Or the pregnancy, the same thing.

Mr. Steyer. Right, or the pregnancy.

So I think very strict and clear limits and guardrails around that are absolutely critical to a strong privacy law. I think everybody on both sides of the aisle would agree with that. And again, the more you guys can make that clear to your colleagues but also to the public, the more we will all win.

Senator Rosen. And would you think since there is such a strong economic benefit to the monetization of your data, that there should be strong economic sanctions if violations occur?

Mr. Steyer. I would. And the only thing I would just say is the big thing to simplify it is the business model is everything. So if you really want to understand how the companies behave—because remember, the technology industry is not monolithic—you really have to take them company by company. It is all about the business model. So if their business model is based on monetizing your personal information through ads, you are going to have to restrict those companies much more.

Senator Rosen. What about using new technology? So you have a smart car. You are going to drive by a certain coffee shop or grocery store every day. Do they say, well, this person drives by there? That is kind of your location. That is your passive usage——

Mr. Steyer. If I opt in. If I opt into that, but give the consumer the right to opt in, not force them to opt out.

Senator Rosen. Thank you. I appreciate it and yield back my time.

The Chairman. Thank you very much.

Senator Blumenthal.

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

Senator Blumenthal. Thank you, Mr. Chairman. And thank you for having this hearing with these very expert and knowledgeable witnesses.

I have heard a lot of worries about the ongoing effort, and I am a part of it in the Congress to frame Federal standards that will protect privacy. I have asked one panel after another whether the people of the United States should have less privacy protection than California. Nobody believes they should. And I assume nobody on this panel thinks that the people of the United States deserve less privacy protection than the people of California. Correct?

Mr. Steyer. Correct.

Mr. Polonetsky. Correct.

Senator Blumenthal. Thank you.

At the same time, there is a legitimate fear that we would either inadvertently or maybe inadvertently undermine State protections. I think that is a real danger, and I would oppose any effort that pre-empts State laws so as to weaken protection for consumers. And I think we are all—or we should be—on guard against that danger.

I know that businesses want a common definition and consistent rules. I also understand some of the criticisms of the California law. Some of that criticism smacks of opposition to the protections
and the substance of those safeguards for consumer protection. Federal rules simply cannot be an opportunity to weaken a strong framework that industry resists or opposes. We can learn from California. We have to provide at least the same standards. In fact, I believe they ought to be even more rigorous and more protective.

So let me ask particularly Mr. Steyer and Ms. Guliani if Congress fails to act now, are other states likely to successfully pass similar bills in the near term. What is on the horizon?

Mr. STEYER. So I can speak to that. I would say I believe Senator Cantwell knows the State of Washington just considered a fairly—it was a different version of the bill and it died. It is the only one that is on the table right now.

So barring action by the Congress, the California law goes into effect in January 2020. It will essentially become the law of the land, and I believe that the tech companies understand that. When we were writing it, we were aware of that. I do not think you are going to see this hodgepodge, mishmash.

And to your point, Senator Blumenthal, the people who are really pushing preemption are primarily certain tech companies that want to weaken the California law. So your point of view of that as a floor that we should build upon for a strong, comprehensive Federal law is I think a very good framework.

Senator BLUMENTHAL. A floor, not a ceiling.

Mr. STEYER. It is absolutely a floor, not a ceiling. And I think there are some very smart folks on this Committee who can build an even better law.

Senator BLUMENTHAL. First do no harm.

Mr. STEYER. Exactly.

Ms. GULIANI. And if I could just speak to that point specifically. I mean, I think particularly in the area of technology, we are talking about rapid changes, and states have shown themselves to be more nimble and adapt to responding to those rapid changes. So what I really fear is a Federal regime that ties State hands, and when new technologies pop up, new problems pop up, we see gaps in a Federal framework that they are not able to address those problems. And I think particularly in an area where when it comes to consumer rights and consumer privacy, states have a long history of expertise and a long history of leading on these issues.

Senator BLUMENTHAL. Well, I share your predilections about the importance of State action, having been State official for about three decades and including two decades as State Attorney General in Connecticut. And both in terms of being more nimble and also closer to their constituents and sharing the effects—we share the real life effects of privacy invasion—I think State officials are a ready and willing source of wisdom on this topic. And so I think we need to be very, very careful in what we do here that may in any way supplant what they are doing.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Sinema.
Senator Sinema. Well, thank you, Mr. Chairman, for holding this hearing.

Data privacy is an important topic for all Americans, and I am glad the Committee continues to explore this complicated issue from all angles. Every day we learn about new misuses of Americans' private data on the Internet, including recent examples in the past month of millions of social media passwords being stored in an unencrypted format.

So this issue requires bipartisan solutions that protect the privacy and security of Arizonans while allowing innovation, creativity, and investment to flow into new and emerging technologies and businesses.

I am particularly pleased this hearing focuses on the impact of data privacy legislation on consumers. They are the ones whose lives get upended if passwords get hacked or identities get stolen. And consumers should have the right to control their own private information.

A particularly vulnerable population to privacy abuses and identity theft are elderly Americans. The United States has COPPA, a specialized privacy law to protect children, but our seniors also experience elevated risks of having their data misused. Elderly Americans sometimes struggle to navigate the complexities of privacy policies, and they are often the targets of fraud. I want to make sure that any Federal privacy law gives seniors in Arizona and across the country the tools they need to thrive in the digital economy and the protections they need to enjoy a productive and secure retirement.

My first question is for Mr. Steyer, but I welcome the perspective of all of our witnesses. So thank you for your focus on children and the particular concerns they face. I think the consumer education piece is a critical aspect of any data privacy legislation. As you state in your testimony, many people who want to limit data collection by websites do not know how to do it, which is an issue of both transparency and digital literacy.

Can you give a brief overview of your digital citizenship curriculum and discuss whether you think any of these tools are appropriate or could be adapted to educate older Americans?

Mr. Steyer. Yes. I think that is a great question, Senator Sinema.

So our digital literacy citizenship curriculum—75,000 member schools now—is basically driver's ed for the Internet and cell phones. It is sort of the basic rules of the road. I think your point about seniors is a great one because they did not grow up with the technology. It is hard for teenagers who are first generation native technology users to understand some of this stuff. So why should a senior citizen?

So I think the importance of consumer education in simple clear ways to understand what your rights are and then how to exercise them—it is basically digital literacy. And if you guys put this into the bill, we will create a curriculum for you for all age ranges in the country.
Mr. Polonetsky. Senator, I would love to see the FTC really taking a lead role. They have a business outreach department. We do a lot of work in Europe. The challenge, frankly, has been the huge number of small businesses that are sending questions, that are sending e-mails that they do not need to send to ask for permission. It has been a big transition. And if we are going to pass a new law—and I hope we do—we should be ready to help the teacher who is creating an app because she thinks it is a better way to teach her kids so that she does not have to hire outside counsel. And I think the FTC, certainly Common Sense, and other groups, but I think the FTC, in addition to giving them those enforcement staff, giving them those education, outreach is critical.

Ms. Guliani. I would just like to make a point. I think that the onus should not be on the individual. Right? I think your question sort of speaks to a larger problem which is the complexities and difficulties that not just elderly Americans but everybody faces. And I think that that is one of the reasons that we have supported an opt-in framework instead of an opt-out. When you talk about technical literacy, the difficulty someone may have in figuring out not only all of the apps they do business with, all of the entities that might have their data, but how to navigate the complex framework of opting out is just too much of a stress to put on consumers. That is why we have supported opt in.

Senator Sinema. Thank you.

Ms. Dixon. I would agree that you should not put too much emphasis in terms of the responsibility of the individual solely to protect themselves, but I think consumer education is very important. The Data Protection Commission in Ireland has just closed a consultation in relation to children and the exercise of their rights under the GDPR, and we consulted directly with children through schools. We developed lesson plans, which was in part an education of children around the uses of their personal data. So we very much believe in active communication to consumers through our website, through the promotion of case studies promoted by the media. And I think this is an important part of the jigsaw as well.

Senator Sinema. Thank you.

Thank you, Mr. Chairman.

The Chairman. Thank you very much.

Senator Sullivan.

STATEMENT OF HON. DAN SULLIVAN,
U.S. SENATOR FROM ALASKA

Senator Sullivan. Thank you, Mr. Chairman.

And I apologize to the witnesses for my late arrival, but I wanted to make sure I was able to ask at least a few questions on very important topic. And what I want to do—and again, if this has been covered, I apologize, but I wanted to focus a little bit more on the international aspects.

We had a hearing, actually a subcommittee hearing, that I chaired yesterday with Senator Markey after our leader here set up a really important new subcommittee on economics and security. And the idea was kind of international standards and where we have typically led in this area—the United States—the NIST Direc-
tor was there and a number of other witnesses at the subcommittee hearing.

But how are we suppose to think through as we look at these privacy standards and the different standards internationally? Obviously, there is what is going on in Europe. But there are also concerns that I have even more broadly than just what is happening in Europe is that when you have kind of the 5G race that is happening globally and Huawei in some ways leading that, that you might have a de facto leadership that relates to standards coming from China that, to be honest, in the world of privacy is a real concern. I think even a bigger concern than the European regulatory framework.

So how should we be thinking about this and trying to help make sure that what we are doing with our allies is the standard that we think is appropriate for countries like ours that are democratic capitalist countries?

Mr. STEYER. Senator Sullivan, if I may, just two points.

Senator SULLIVAN. Please and I open this up to all.

Mr. STEYER. A couple of points.

One, when we wrote the California law last year, the CCPA, which we have been talking about in the hearing, we met the folks who wrote GDPR, and we realized that the values of the U.S. are in many ways similar to folks in the EU, but they are different in certain areas. So we were very careful—and I think that this could be done here at the Federal level as well—to think about how there are certain areas like the First Amendment—we were talking about this earlier—that may mean that a privacy law in the United States would be slightly different than GDPR. But most of the protections are universal.

That said, you can modify——

Senator SULLIVAN. Universal relative to liberal democracies?

Mr. STEYER. That is what I was going to say.

And the second thing is I would be willing to bet you a large sum of money that Huawei will not dominate the 5G universe, and I mean that.

Senator SULLIVAN. Why? I am glad you are so optimistic.

Mr. STEYER. Because the technology in the United States and the companies in the United States have brought this world extraordinary advances. That does not mean we do not need to be aware of this, but sacrificing important privacy protections for consumers just because China might do that would not be a smart strategy. And I think at the end of the day, a strong Federal privacy protection where the California law is the floor and where you really take into consideration the fact that most of the companies that matter are here in the United States will give us the protections that we need.

Senator SULLIVAN. Other thoughts?

Ms. GULIANI. I was going to say, I mean, I think that we can take some good lessons from GDPR. Regulation in the U.S. is not going to look exactly the same as Europe. There are concerns with the right to be forgotten and changes that would need to be made to be consistent with the U.S. Constitution. The enforcement framework will look different. And also in the U.S., we have State-level actors, attorneys general, agencies, legislatures, and I think
the last thing we want to do is weaken the ability of those actors who have a long history of working on these issues of sort of having a seat at the table and being able to enforce and create good laws.

But having said that, there are positive elements of GDPR that we should take and learn from, the extent to which it places rights in the hands of consumers and increases standards around consent, and limits on how——

Senator SULLIVAN. Let me just real quick and then I would like to hear the rest. But none of you are advocating for a state-by-state approach to this. Are you?

Mr. STEYER. No, but we were very clear we have deep skepticism about preemption if there was going to be a watered-down Federal law that would, say, lessen the protections you have at the baseline of California. So that was the discussion we had earlier.

Mr. POLONETSKY. Just to look to the Asia-Pacific allies that we do have. So we have had a leadership role in the APEC process where we have worked with Japan, Korea, a number of the major economies who similarly want to cooperate with data protection flows. You will be considering the new NAFTA treaty. We committed to use the APEC CBPRs, the APEC process to move data across North America. So GDPR, obviously, is an important place-setter, but we have been a leader in OECD, which has an important set of privacy frameworks, and we have been very active throughout many administrations in the APEC process, and those are two regimes we should look to for global cooperation.

Senator SULLIVAN. Great.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Sullivan.

There is a vote on. Senator Cruz is recognized and will preside for a time. Senator Cruz.

STATEMENT OF HON. TED CRUZ, U.S. SENATOR FROM TEXAS

Senator CRUZ [presiding]. Thank you, Mr. Chairman.

Thank you to each of the witnesses for being here.

There is no doubt that protecting privacy is critically important, and how we should do so, what government regulation should be in place concerning privacy is going to be a policy question that I suspect will be with us a very, very long time.

At the same time that we want to protect privacy, we also want to avoid a regulatory system that imposes unnecessary burdens and that threatens jobs. And I think there are lessons that we can draw based on the experience we have seen elsewhere.

There has been considerable discussion here about the European Union’s General Data Protection Regulation, GDPR. In November 2018, the National Bureau of Economic Research found that, quote, the negative effects of GDPR on technology investment appear particularly pervasive for nascent 0 to 3-year-old ventures, which may have cost European startups as many as 39,000 tech jobs.

Even more alarming, the report goes on to state, quote, the potential for job losses may well extend and intensify past our four months post-GDPR dataset period, in which case the effects on jobs is understated.
In the wake of GDPR, California enacted its own law, the California Consumer Privacy Act of 2018. And according to the International Association of Privacy Professionals, the California Privacy Act will affect more than 500,000 U.S. companies, the vast majority of which are small to medium sized enterprises.

What lessons should this committee or should Congress take from the experience with GDPR and the experience with the California Privacy Act?

Mr. STEYER. So, Senator Cruz, I am Jim Steyer and we basically wrote the California privacy law with the legislature there.

I would tell you the bottom line lesson is that privacy is good for business. We wrote that law really with some of the most important tech companies in the United States, Apple, Microsoft, SalesForce. But I run a small business with several hundred employees. We have to comply with the California law and GDPR. And so I run a small business and know the fact that it does matter.

But in the long run, I think what you saw was you had unanimous bipartisan support in California among all the Republican legislators, as well as Democratic legislators to support it.

So I would just say well crafted, strong privacy protections are in the best interest of business. And I think that the record speaks for itself in that regard, and you should feel confident that a smart California legislature, will find the right balance on that.

Senator CRUZ. So let me focus for a second on the GDPR piece. Do the witnesses agree that the GDPR regulation is having or had a significant negative effect on jobs? And are there lessons that we should derive from that?

Mr. POLONETSKY. I think, Senator, one easy lesson that we can take and improve on, as we look how to legislate in the GDPR, the European Data Protection Board is issuing quickly—but frankly, it is a year in—opinions on some of the core protections of the GDPR. There is an opinion out now that is not yet final on what can be in a contract. And obviously, that is a core thing. Lots of companies are doing their business based on contract. And we will not have final guidance and it is a year out.

Ms. GULIANI. And I do not think it is necessary that a privacy law is going to hurt small businesses. I do think that a law should reflect the realities of small businesses. So, for example, penalties. You might want to have different penalties based on the size of a business or the amount of data they hold.

And I do think there are some rumors and myths around the extent to which GDPR harms some businesses. I will give you a good example that has been reported. Following GDPR, the “New York Times” reportedly stopped doing targeted advertising in Europe and did contextual advertising. They did not find that their advertising dollars went down. They went up. And so I do think that
there are ways that businesses can respect privacy and make a profit. And we are starting to see businesses that are innovating around that. DuckDuckGo, who is trying to create an alternative to Google that respects privacy. So this is also an industry to, I think, promote privacy and create rights-respecting products.

Mr. STEYER. And, Senator Cruz, I would tell you that we have been spending a fair amount of time talking about the incredible importance to your family, my family, and everybody in this room’s family, and ourselves about the protections. Living in the state where most of the big and small tech companies are based and working with them, I think they have now come to the conclusion that while there may be some modifications that need to be made, which is the normal legislative rulemaking process, in the long run this is good for business and it is good for consumers. It is good for everybody.

So I agree with Ms. Guliani that I think some of the statements about job losses have been overstated and that the value of a quality privacy regime for the Cruz family, the Steyer family, and everybody else is totally worth it.

Ms. DIXON. Senator, equally at the Irish Data Protection Commission, we are not aware of evidence that the GDPR is affecting jobs adversely. I spoke earlier about the risk-based approach that the GDPR endorses, and it does give a nod to smaller and micro-enterprises and it provides for implementation only of the organizational and technical measures that are appropriate and proportionate to the risks of the personal data processing operations in question and to the scale of the organization. So I think approached and implemented as it is intended, it should do the opposite of affect jobs. It should engender better consumer trust and a more sustainable business model.

Senator CRUZ. Well, I want to thank each of the witnesses for your testimony. This testimony has been helpful.

The hearing record will remain open for two weeks. During that time, Senators are asked to submit any questions for the record. And upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible, but no later than Wednesday, May 15, 2019.

With that, I thank each of the witnesses for testifying, and the hearing is adjourned.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]
Question 1. Your testimony highlighted obligations placed on organizations operating under the GDPR as a “series of high-level, technology neutral principles,” such as lawfulness, fairness, and transparency, among many others. Would you please explain the significance of any future regulatory privacy framework maintaining a technology neutral approach?

Answer. The significance of a technology-neutral approach in any future regulatory privacy framework is that the law would remain adaptable to govern any type of personal data processing scenario and in any context. Equally, the law would not require frequent updating to keep pace with technology and terminology changes in areas technologies that cannot easily be anticipated in advance.

The flip-side of this capability of the law to remain adaptive to new technologies is that, in enforcing the law, supervisory authorities cannot start from a point where they are applying a very prescriptive and context-specific standard set down in the law. Rather, enforcers must go back to first principles and examine the technological features and context of any given set of personal data processing operations and decide whether there is compliance with the principles. So, for example, facial recognition as a technology is not referenced directly in the GDPR and nor are any use cases involving facial recognition prohibited. The enforcer in examining a complaint about facial recognition would have to examine whether the requirements and conditions for processing of special categories of data (biometric data is a special category under GDPR) are met in each very specific implementation context. This means investigations of issues require the time for in-context analysis prior to any enforcement action.

Question 2. Your testimony briefly described the “rights of consumers” set out in Chapter 3 of GDPR, and you specifically mentioned the “varying conditions pertaining to the circumstances...[that] those rights can be exercised.” Based on your interpretation of the right to data portability, are there unique circumstances or factors that determine when this particular right should be exercised? Are there certain circumstances in which portability requests are not appropriate to execute?

a. Given relevant competition concerns inherent in the portability requirement, are there special considerations taken into account for compliance determinations in regards to the right?

Answer. The reference to the varying conditions under which the right to portability can be exercised was a reference to the fact that it applies only to data which has been collected under the legal bases of consent or contract. It applies only to the personal data provided directly by the user or to observed data flowing from the user actions. It does not apply to inferred data. I attach for the Senator’s information an opinion of the European Data Protection Board interpreting and clarifying the right to portability which may be useful.

An aim of the right is that it will ultimately lead to the fostering of more consumer services and choice for users. Any scenario where an organisation asserts a commercial or confidentiality sensitivity or a risk of prejudicing of third party rights in delivering portability would be examined on its merits by the Data Protection Commission.

We are certainly in the early days with regard to full implementation of this right. Early initiatives such as this one implemented by some of the major platforms shows the direction of travel to-date with online service providers:

https://datatransferproject.dev/

Question 3. In March, my Subcommittee on Consumer Protection held a hearing focused on the specific concerns of small and new businesses that operate in different sectors and how they utilize and protect consumer information in their operations. These businesses have fewer resources in handling the complexities of increased regulatory privacy compliance and associated costs. Additionally, not all
businesses are the same, and consumer data offers different uses, challenges and, in some cases, liabilities, across the various models of small businesses and start-ups. How does the Irish Data Protection Commission account for small and new businesses in its enforcement actions aligned with GDPR?

Answer. SMEs (Small and Medium Enterprises) make up over 99 percent of businesses in Ireland with a significant proportion of that figure being categorised as micro enterprises. It was therefore a considerable focus of the Irish Data Protection Commission in the run-up to the application of the GDPR in May 2018 to ensure that small business concerns were addressed and that there was clarity in terms of what was anticipated regarding their implementation of GDPR.

A year prior application (May 2017), the Data Protection Commission procured an independent survey of small businesses to assess their level of awareness and understanding of the new law. This allowed us focus our support initiatives in specific ways. We engaged extensively with representative bodies of small businesses and worked with them on drawing up and publishing and promoting simple "12 Step Guides" on how to commence preparations. We developed a micro site (now removed) www.gdprandyou.ie which we populated with guidance materials. We engaged with specific sectors directly through seminars and workshops clarifying the risk-based approach endorsed by the GDPR. The Data Protection Commission rolled out an extensive media campaign that also covered cinemas in Ireland to promote awareness and to direct small business owners to our micro website. We increased staffing on our caller helpline in order to be available to answer queries from small businesses directly.

When we re-ran the survey with SMEs in March 2018, awareness levels had jumped significantly and small business confidence in preparation for the new law had increased considerably.

In terms of the fact that small businesses vary greatly from one another as concerns their types of data use, we communicated heavily that the approach that needs to be taken starts with a risk-assessment and ultimately implements organisational and technical measures appropriate to the risk. Several of the provisions of the GDPR in many cases do not apply to small businesses: for example, the Article 30 requirement to document data processing activities or the Article 37 requirement to appoint a Data Protection Officer may equally not apply.

In terms of enforcement, the Irish Data Protection Commission mirrors the risk-based approach of the GDPR and targets enforcement activity at the areas of highest risk and which impact the most users. In the majority of cases currently involving smaller businesses, we will seek to mediate between a complainant and the business to amicably resolve any complaints about data protection we receive, ensuring as we do to educate the small business on where its compliance efforts may need to be stepped up.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO JULES POLONETSKY

Question 1. Are you concerned that overly broad purpose limitations could negatively impact research, including research related to artificial intelligence?
a. Do you have similar concerns about overly broad consumer deletion rights?

Answer. Thank you for considering the many beneficial opportunities to use some types of data for research purposes. General agreement on use limitations commonly allows for the inclusion of research for product improvement and related product development as “reasonable expectations,” which in recent years may include research, training or testing on machine learning models. We see this at an increasing rate as more and more products, services, features, and new technological capabilities are built on AI and ML systems.

Research conducted to develop or improve entirely new or unrelated products is arguably not expected in this sense, and could be beyond the scope of what a consumer intended when originally providing the data. This might be particularly true for data processed using machine learning, as it may not be possible to identify sufficiently broad secondary use cases at the time of collection. In some cases, data may be de-identified, but in other situations this may not be feasible. In some circumstances, the new use creates no risk to individuals and should not be of concern. This is where an ethics review process, recognized by law, would be valuable. For example, for researchers subject to the Common Rule, this use of data for academic human subject search would go through review by an Institutional Review Board, where informed consent might be required as well as other protections. Or the Board might waive consent, after weighing the risks, benefits, and ethical concerns. FPF and other leading scholars have called for the creation of such review proc-
esses, which can be used by companies and academics conducting research on data that is outside the Common Rule IRB framework. We believe such a trusted process will be essential for assessing uses of data when informed consent is not feasible.

Thank you for asking about an important aspect of many privacy laws and bills, which provide consumers with the opportunity to delete their data in appropriate contexts. In some cases, this is not an option. Based on existing regulatory requirements, a bank customer cannot request deletion of his bank records, even if he closes his account. Likewise, academic, medical, and other business related records may have independent requirements that limit a consumer's right in this area. When this is the case, sufficient leeway should limit the deletion rights to allow necessary retention. In other cases, for example, engagement with social media, or other discretionary interactions with individual organizations, an individual should reasonably be able to delete her information and rely on that erasure. To the extent that such data has already been included in aggregated or de-identified datasets, there should be no conflict between the deletion of personal data, and the retention of those datasets for further analysis or use to train machine learning models. In addition, the requirements for sufficient breadth and diversity of data in these training datasets might be impacted (that is, they may become unacceptably biased, or insufficiently representative) if individual records are required to be removed. In cases of particularly sensitive data where removal of an individual's record might be desired or required, additional strategies could be employed to ensure the validity of the dataset is retained. An example would be applying differential privacy strategies, which allow evaluation of a dataset both with, and without, an individual record, to ensure that analysis on that dataset remains consistent.

Question 2. Your testimony thoroughly describes ten privacy-enhancing technologies, or PETs, that can "achieve strong and provable privacy guarantees while still supporting beneficial uses" of data. Do you have specific recommendations for this Committee as to how Federal legislation could incentivize the growth and development of new PETs?

Answer. Thank you for asking about the benefits of privacy-enhancing technologies (PETs). Providing organizations with incentives to implement PETs is one of the most important things a Federal privacy law can do to improve consumer privacy while promoting beneficial uses of data. There are several legislative tools that could provide incentives for organizations to employ PETs.

FPF has proposed that legislation recognize several tiers of personal information and tailor resulting rights and obligations based on the identifiability of the data, given the technical and legal controls that are applied. We propose a strong standard for covered data that would include a broad range of data that is linked or can practicably be linked to an individual. Within this range, we propose that lawmakers can provide for a degree of latitude for compatible uses when data is pseudonymized and non-sensitive. When data is pseudonymized and sensitive, we suggest that there be some but less latitude. Finally, we recognize that some technical methods can result in data being considered de-identified. These tiers would provide incentives for companies to apply technical de-identification to data, as opposed to binary proposals that treat data as either included or excluded from regulation.

In addition to nuanced legislative definitions, a Federal privacy law can provide other direct incentives to employ PETs:

- A law could create safe harbors for certain PETs-protected activities. For example, a law could designate some data as "not identifiable" (and thus subject to few or no consent obligations) when the organization employs on-device differential privacy to ensure that aggregate data about user behavior cannot be reliably linked to individuals.
- A law could create rebuttable presumptions regarding data safeguarded by PETs. For example, a law could establish a presumption that an organization meets the law's security requirements with regard to data that is encrypted using robust cryptography and also protected by a comprehensive data security program.
- A law could reduce some legal obligations in order to promote practical privacy protections. For example, a law could reduce transparency or choice requirements when organizations use homomorphic encryption to reduce or eliminate third parties' ability to identify individuals during routine commercial transactions like retail purchases, online advertising, or marketing attribution.

In addition to providing the FTC with greater enforcement resources, a Federal law can direct additional funding to the FTC's Office of Technology Research and Investigation. As a key part of the FTC's education efforts for legal compliance, es-
especially for small businesses, the FTC should also research emerging de-identification technologies in order to be aware of their strengths and weaknesses, and hold workshops that provide opportunities for discussion and debate over the efficacy of emerging PETs.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JERRY MORAN TO NEEMA SINGH GULIANI

Question. Similar to what your testimony stated, I have heard from many interested parties that the FTC currently lacks the resources needed to effectively enforce consumer privacy under its current Section 5 authorities. As a member of the Senate Appropriations Subcommittee with jurisdiction over the FTC, I am particularly interested in understanding the resource needs of the agency based on its current authorities, particularly before providing additional authorities. Do you have specific resource-based recommendations for this committee to ensure that the FTC has the appropriations it needs to execute its current enforcement mission?

Answer. The FTC needs additional resources for enforcement to enable it to act as an effective watchdog. In the last 20 years, the number of employees at the FTC has grown only slightly. And the number of employees in the Division of Privacy and Identity Protection (DPIP) and the Division of Enforcement, which are responsible for the agency’s privacy and data security work, stands at approximately 50 and 44 people, respectively. In addition, the FTC needs additional technical expertise, so that it can adapt to changes in technology. For example, technologists and academics have found that advertising companies “innovate” in online tracking technologies to resist consumers’ attempts to defeat that tracking, frequently using new, relatively unknown technologies. It is unclear whether the agency has the technical capacity to keep pace with such innovations. A more detailed review of how the commission is currently allocating its existing resources is needed to assess whether there are additional areas where existing resources should be augmented.