

1 BEFORE THE NEW YORK STATE SENATE
2 STANDING COMMITTEE ON CONSUMER PROTECTION
3 AND
4 STANDING COMMITTEE ON INTERNET AND TECHNOLOGY
5 -----

6 JOINT PUBLIC HEARING:

7 TO CONDUCT DISCUSSION ON ONLINE PRIVACY,
8 AND WHAT ROLE THE STATE LEGISLATURE
9 SHOULD PLAY IN OVERSEEING IT
10 -----

11 Hamilton Hearing Room B
12 Legislative Office Building, 2nd Floor
13 Albany, New York

14 Date: June 4, 2019
15 Time: 10:00 a.m.

16 PRESIDING:

17 Senator Kevin Thomas, Chair
18 Senate Standing Committee on Consumer Protection

19 Senator Diane Savino, Chair
20 Senate Standing Committee on Internet and Technology

21 PRESENT:

22 Senator John Liu

23 Senator Jamaal T. Bailey
24
25

	SPEAKERS:	PAGE	QUESTIONS
1			
2			
3	Zachary Hecht	8	28
4	Policy Director		
5	Tech NYC		
6			
7	John Olsen	8	28
8	Director, State Government Affairs,		
9	Northeast Region		
10	Internet Association		
11			
12	Christina Fisher	8	28
13	Executive Director, Northeast		
14	TechNET		
15			
16	Ted Potrikus	8	28
17	President & CEO		
18	Retail Council of New York State		
19			
20	Ari Ezra Waldman	65	89
21	Professor of Law		
22	New York Law School		
23			
24	Lindsey Barrett	65	89
25	Staff Attorney & Teaching Fellow at		
26	Institute for Public Representation		
27	Georgetown University Law Center		
28			
29	Joseph Jerome	65	89
30	Policy Counsel		
31	Center for Democracy and Technology		
32			
33	Mary Stone Ross	65	89
34	Co-author of		
35	California Consumer Privacy Act		
36	MSR Strategies		
37			
38	Allie Bohn	130	140
39	Policy Counsel		
40	New York Civil Liberties Union		
41			
42	Charles Bell	130	140
43	Programs Director		
44	Consumer Reports		
45			
46			
47			
48			
49			
50			

	SPEAKERS (continued):	PAGE	QUESTIONS
1			
2			
3	Kate Powers	152	
4	Director of Legislative Affairs		
5	NYS Attorney General's Office		
6			
7	James Loperfido	158	180
8	Vice President of BD, North America		
9	Soramitsu Co., Ltd.		
10			
11	Marta Belcher	158	180
12	Attorney		
13	Ropes & Gray, LLP		
14			
15	John T. Evers, Ph.D.	158	180
16	Director of Government Affairs		
17	The Business Council of NYS, Inc.		
18			
19	Andrew Kingman	158	180
20	Senior Managing Attorney		
21	DLA Piper, LLP		
22			
23			
24			
25			

---oOo---

1 SENATOR THOMAS: Good morning, everyone, and
2 welcome to the first joint hearing of the Senate
3 committees on Consumer Protection, and, Internet
4 Technology.

5 I am joined by the Chair of Internet and
6 Technology, Ranking Member -- I'm sorry,
7 Diane Savino.

8 And I have Senator John Liu here with me as
9 well.

10 We are holding this hearing because there has
11 been major data breaches and widespread misuse and
12 unauthorized sharing of consumers' personal data.

13 In this modern age we live in data is gold.

14 Our apps need it, our websites need it. It
15 makes our lives easier by allowing us to communicate
16 better and conduct business faster.

17 But there is an unexpected cost to this, and
18 that is our personal information, and how it is now
19 traded like a commodity without our knowledge.

20 Legal notices in apps we use everyday are
21 only intended to disclose the positive uses of
22 personal information collected, but they take long
23 to read and is even longer to understand.

24 The positive uses of data by companies
25 include needing personal information to deliver a

1 package or a charge for a service.

2 Some data is used for research and
3 development of new products and improving services.

4 Sometimes it's used for fraud prevention or
5 cybersecurity purposes.

6 In reality, some of the information being
7 gathered is also being shared in ways we cannot even
8 imagine.

9 Data use results in discrimination,
10 differential pricing, and even physical harm.

11 Low-income consumers may get charged more for
12 products on-line because they live far away from
13 competitive retailers.

14 Health-insurance companies could charge
15 higher rates based on your food purchases or
16 information from your fitness tracker.

17 A victim of domestic violence may even have
18 real-time location-tracking information sold to
19 their attacker.

20 These are simply unacceptable uses of
21 people's data.

22 We cannot get around the fact that we are
23 living in a data-driven world, and things need to
24 change.

25 That's why we are here today for this

1 hearing.

2 We will hear from experts from industry,
3 government, and advocates about what a strong set of
4 standards should look like.

5 We can give New Yorkers their privacy rights
6 and allow our economy to thrive.

7 I'm looking forward to gathering the guidance
8 from all five panels today.

9 And I'm going to now yield my time to
10 Senator Savino.

11 SENATOR SAVINO: Thank you, Senator Thomas.

12 And I'm happy to join Senator Thomas and
13 Senator Liu; Senator Thomas, of course, Chair of the
14 Consumer Committee, at this joint hearing.

15 As he said, we're here to discuss online
16 privacy, and what role the Legislature and the
17 government should have in it.

18 As we all know, the Internet and technology
19 reaches into all facets of our lives these days, and
20 into many committees in the Legislature.

21 While the particular pieces of legislation
22 we're discussing today are in the Consumer Affairs
23 Committee, they are of interest to the Internet and
24 Technology Committee. As you all know, we now have
25 a new Senate standing committee.

1 The government is probably a decade behind in
2 beginning to examine some of these issues and help
3 develop public policy around them.

4 And it's important that we have hearings like
5 this, taking testimony from experts who can help us
6 develop sound public policy to regulate in a smart
7 way; not overreach, not stymie development, but
8 really delve into what we should and shouldn't do on
9 the government side.

10 So I look forward to hearing from you today
11 as we begin to tackle these complicated issues, like
12 data privacy, and how it affects all of us.

13 Thank you.

14 SENATOR THOMAS: Senator Liu, do you have...

15 SENATOR LIU: I will thank you,
16 Mr. Chairman.

17 And I will only say, I am very happy to see
18 that this hearing is taking place.

19 I want to thank Chairs Thomas and Savino for
20 convening this. Online privacy is a big issue, and
21 it's getting bigger.

22 I hear it from my constituents. I hear it
23 from, pretty much, everybody.

24 It's a fact of life now, that we have to be
25 worried about our online privacy, our information

1 that is online, and, certainly, when the information
2 is being bought and sold, as Senator Thomas
3 mentioned, often without our knowledge.

4 So I look forward to hearing these experts,
5 and helping to craft legislation that will help all
6 New Yorkers.

7 Thank you.

8 SENATOR THOMAS: With that being said, we
9 have the first panel here.

10 Forgive me if I slaughter any of your names.

11 We have from the Retail Council of New York
12 State, Ted Potrikus;

13 We have from TechNET, Christine Fisher;

14 We have from Tech New York City;

15 Zachary Hecht;

16 And from the Internet Association, my good
17 old friend, John Olsen.

18 All right, so, rules before we start here.

19 The entire panel, you know, is given
20 20 minutes; so each of you have five minutes to,
21 basically, you know, talk about your testimony.

22 You don't have to read, you can summarize.
23 And then all three of us, and more, can ask you
24 questions.

25 All right?

1 So with that being said, you know, just
2 start; whoever wants to start, may start.

3 ZACHARY HECHT: Chairman Thomas,
4 Chairwoman Savino, and members of the two
5 committees, thank you for calling this exploratory
6 hearing, and for the opportunity to testify.

7 My name is Zachary Hecht, and I'm the policy
8 director at Tech NYC.

9 In my testimony today, I'll voice support for
10 S5755, the SHIELD Act; and also detail our
11 opposition to S5642, nominally, the New York Privacy
12 Act.

13 While the SHIELD Act would serve to benefit
14 New Yorkers, S5642 would negatively impact
15 New Yorkers and have serious repercussions for
16 New York's economy.

17 Tech NYC is a nonprofit coalition, with the
18 mission of supporting the technology industry in
19 New York through increased engagement between our
20 more than 750 member companies, New York government,
21 and the community at large.

22 Tech NYC works to foster a dynamic, diverse,
23 and creative ecosystem, ensuring New York is the
24 best place to start and grow technology companies,
25 and the New Yorkers benefit from the resulting

1 innovation.

2 As technology proliferates and plays an
3 increasing role in our everyday lives, there has
4 been a growing international conversation around
5 data privacy and security.

6 We welcome this conversation, as protecting
7 consumers is not only the right thing to do, but
8 also an increasingly crucial component of commercial
9 success.

10 Privacy is becoming a core business function
11 for many technology companies, and a number of
12 researchers at companies and in academia are
13 developing privacy-enhancing technologies.

14 Advances in encryption, federated learning,
15 secure multiparty computation, differential privacy,
16 and other areas, allow technology companies to
17 continue offering innovative services while ensuring
18 privacy.

19 And while many technology companies are
20 committed to ensuring data privacy and data
21 security, it is also clear that government has an
22 important role to play in protecting consumers.

23 The technology industry, and, our society,
24 more broadly, are facing real questions how data is
25 collected, used, and shared.

1 These are hard questions to which there are
2 no easy answers.

3 The Internet and digital technologies have
4 fundamentally changed the way we live our lives, and
5 now is the time for the public sector and private
6 sector to come together to find a path forward.

7 Recently, there have been two notable efforts
8 aimed at increasing consumer-data privacy, both
9 outside the context of the U.S. federal government.

10 The first of these is the EU's GDPR, and
11 that's a comprehensive data-privacy regulation
12 applying to businesses in the EU and businesses
13 collecting or processing the data of EU residents.

14 This has been in effect for over a year, and
15 while it should serve as an important framework for
16 future regulation, there have also been a number of
17 unintended consequences and issues.

18 And the second recent effort to regulate data
19 privacy is the CCPA, which attempts to regulate a
20 set of privacy rights for California residents.

21 CCPA was signed into law in 2018, but is not
22 effective until 2020.

23 In light of all of the recent conversation,
24 we would like to commend the New York State Senate
25 for considering how to best protect New Yorkers, and

1 voice our support for S5575, the SHIELD Act.

2 The SHIELD Act will help heighten
3 data-security requirements and protect New York
4 residents from security breaches.

5 However, we do have serious concerns about
6 S5642, and caution against its advancement.

7 While we recognize the need for increased
8 data-privacy regulation, these types of regulations
9 should generally be enacted on the federal level.

10 Simply put: The Internet transcends state
11 borders, and a state-by-state patchwork of
12 regulations creates a complex compliance regime, and
13 makes it difficult, if not impossible, for small
14 companies to compete.

15 The U.S. Senate is actively discussing and
16 drafting privacy legislation, and may issue a
17 bipartisan proposal very soon.

18 New York should allow the federal government
19 to take the lead here.

20 Beyond the fundamental issue of
21 state-by-state approach to privacy, S5642 contains a
22 number of ill-advised provisions.

23 It copies measures from GDPR and CCPA, but
24 does nothing to ameliorate the shortcomings of those
25 regulations, and it results in substantial negative

1 consequences for tech companies and non-tech
2 companies and individual New Yorkers.

3 Some of the negative consequences are:

4 High-compliance costs for businesses of all
5 types and sizes;

6 Decreased economic growth for New York;

7 Increased online security risks;

8 And chilling effects on free speech and free
9 expression.

10 In the remainder of my testimony I'll break
11 these down quickly.

12 S5642 would require almost every business to
13 spend a significant amount of resources and money on
14 compliance.

15 The litany of new consumer rights established
16 would require businesses to fundamentally rework
17 their internal processes and establish new systems
18 to accept and fulfill consumer-data requests.

19 Complying with S5642 will necessitate
20 significant upfront and ongoing costs, and many
21 businesses may pass these on to consumers, some may
22 stop offering certain services, and others may be
23 forced to close.

24 After GDPR was into effect, there were
25 billions of dollars in compliance costs for

1 businesses in the United States.

2 S5642 doesn't just require compliance from
3 the largest companies. It essentially applies to
4 any business using digital technology to serve or
5 reach their customers, including, small bagel shops
6 on Long Island that use e-mail marketing, or small
7 startups that have one employee.

8 And the difficulty in costs of compliance in
9 this legislation will benefit large companies and
10 disadvantage small businesses, negatively impacting
11 competition and innovation.

12 The large companies will be able to hire
13 compliance staff and spend significant resources
14 reworking products and services, while small
15 businesses will not be able to do the same.

16 Again, we can look to what's happened in
17 Europe since GDPR was implemented.

18 OFF-CAMERA SPEAKER: That is time.

19 JOHN OLSEN: Good morning.

20 My name is John Olsen. I'm the director of
21 state government affairs for the northeast region.

22 I want to thank Chairs Thomas and Savino, and
23 Senator Liu, for allowing me to testify today.

24 IA's mission is to foster innovation, promote
25 economic growth, and empower people through the free

1 and open Internet.

2 The Internet creates unprecedented benefits
3 for society.

4 And as the voice of the world's leading
5 Internet companies, we ensure stakeholders
6 understand these benefits.

7 (Indiscernible) is that understanding as
8 critical to the functionality and vitality of our
9 companies, and in consumer trust; trust in the
10 services our companies provide and trust in the
11 handling of data our users generate.

12 It is IA's belief that consumers have a right
13 to meaningful transparency and full control over the
14 data they provide with respect to the collection,
15 use, and sharing of that data.

16 Consumers should have the ability to access,
17 correct, delete, and transfer their data from one
18 service to another.

19 IA is here today to comment on proposed
20 legislation, and to provide insight from efforts in
21 other states, as well as at the federal level,
22 regarding consumer privacy, and the impacts it has
23 on business in general, and not just Internet-based
24 businesses.

25 I want to first address the proposed New York

1 Privacy Act, Senate Bill 5642, by Chair Thomas.

2 In its current form, Internet Association is
3 opposed to the passage of the bill.

4 Upon review, this bill appears to define
5 provisions from the California Consumer Privacy Act
6 and the European General Data Protection Regulation,
7 and creates a new concept in state law known as
8 "The Data Fiduciary."

9 IA has significant concerns with the way this
10 legislation is structured.

11 The association's primary concerns are as
12 follows:

13 The bill creates highly complicated and
14 problematic definitions for "opt in," "personal
15 data," "sale," and "privacy risk," that captures
16 almost every aspect of the interaction between a
17 business and a consumer.

18 Opt-in requirements apply not just in sale or
19 sharing of personal data, but also the collection
20 and processing of data that is performed by almost
21 every business in 2019.

22 This law will have informed consent applied
23 to nearly all interactions taking place online. It
24 would fundamentally alter New Yorkers' user
25 experience, and, to an even greater degree, in what

1 is being experienced in the European Union under
2 GDPR.

3 In addition, it is important to note that
4 neither CCPA nor GDPR have a blanket opt-in
5 requirement for all data processing.

6 CCPA, instead, allows users to opt-out of the
7 sale of their personal information.

8 The "data fiduciary" concept is unprecedented
9 in its scope, and when combined with the
10 requirement that fiduciary duties with regard to
11 privacy risk supersede duties and obligations to
12 shareholders and owners of private or
13 publicly-traded companies, raises significant
14 First Amendment concerns.

15 Compliance with the requirements of this
16 provision, coupled with the ability for private
17 residents to initiate legal action against companies
18 in violation of data-fiduciary obligations, would
19 bankrupt small businesses, and likely some larger
20 businesses.

21 User trust is fundamental to the success of
22 Internet companies, and responsible data practices
23 are critical for earning and keeping user trust.

24 Any company processing personal data should
25 do so responsibly, acting as a good steward, by

1 taking steps to ensure that data is handled in a
2 manner that conforms to consumers' reasonable
3 expectations.

4 However, enshrined in state law, requirements
5 mandated in Senate Bill 5642 would create an
6 entirely new experience for New York residents while
7 doing little to preserve consumer privacy.

8 This bill would cause significant compliance
9 issues for all businesses, without exception,
10 throughout New York's economy, and would create a
11 competitive advantage for businesses outside of
12 New York's borders.

13 In addition, it would create a new regime, in
14 requiring consumers to review notices, and consent
15 to the collection and processing of their data, by
16 every website, business, online platform, et cetera,
17 creating a negative online experience for users.

18 Imagine the mandated cookie-notice consent
19 ban required in Europe greatly multiplied here in
20 New York.

21 It is important to place the concept with
22 consumer-data privacy in the context of harm. The
23 collection and sharing of personal data that does
24 not include health or financial information has
25 become an essential tool for businesses, large and

1 small, to grow their customer base, tailor their
2 advertising, and provide meaningful feedback to
3 consumers.

4 However, when consumers' private information
5 is inadvertently exposed, or when a significant
6 breach of cybersecurity occurs, it is essential for
7 consumers to be properly informed as to the level of
8 impact of a breach.

9 That is why IA supports the passage of the
10 attorney general's proposed SHIELD Act, Senate
11 Bill 5575A, that would require any business that
12 owns or licenses computerized data to disclose the
13 security breach of a system following discovery or
14 notification of a breach.

15 IA would encourage the inclusion of a
16 threshold for affected parties that is in line with
17 other state breach laws, as well as establishing a
18 standard for notification, access, and acquisition
19 of private information.

20 IA recognizes the need to update New York's
21 data-breach laws, and this legislation would ensure
22 that New York consumers receive timely notification,
23 and help to prevent private information from
24 remaining exposed to potential identity theft and
25 fraud.

1 Thank you for your time, and I'm happy to
2 answer any questions your committees may have.

3 CHRISTINA FISHER: Good morning.

4 My name is Christina Fisher. I am the
5 executive director for the northeast for TechNET.

6 TechNET is a national bipartisan organization
7 of technology CEOs. We advocate at the 50-state and
8 federal level on policies to advance the innovation
9 economy.

10 I thank you for the opportunity to testify
11 today.

12 Before I get into details on some of the
13 proposed legislation that's currently before the
14 New York Legislature, I would like to provide some
15 context, specifically in regards to the General Data
16 Protection Regulation, also known as "GDPR," that
17 was passed one year ago in Europe.

18 TechNET believes that there are important
19 lessons learned from GDPR, and the process that was
20 undertaken in Europe, and think that those could be
21 very helpful in informing the New York State
22 Legislature as you consider legislation this year.

23 First and foremost, GDPR enhances the
24 portability of consumer data while allowing
25 consumers to also correct and delete their data.

1 This is an important concept that our members
2 support, and is very -- it's something that should
3 be considered here in the United States as well.

4 However, there are several lessons learned
5 that we would like to continue to remind the
6 Committee to avoid as we consider legislation here.

7 First and foremost, is to avoid unintended
8 consequences.

9 The easiest way to do this is to allow for
10 time and thoughtful consideration and deliberation
11 around these complex and thoughtful discussions.

12 The European Union allowed for a two-year
13 deliberation between the enactment and when the
14 regulations would be in effect.

15 That allows for businesses to understand the
16 regulations, and allow them to comply, and for
17 countries to be able to make sure that their
18 businesses would be able to comply.

19 By contrast, in California, the CCPA was
20 hastily passed to avoid a problematic ballot
21 initiative. And, as a result, there were several
22 unintended consequences in that piece of
23 legislation. And the effective date of that will
24 allow businesses very little time to comply with the
25 new law.

1 Additionally, as you've already heard here
2 today, there is going to be a dramatic impact on the
3 startup and small-business economy in Europe.

4 Startups have little money to invest in
5 compliance.

6 Since GDPR's enactment, investment has
7 dropped 40 percent in Europe.

8 Additionally, in the United States, an
9 average business of 500 employees costs about
10 \$83,000 in their first year to comply with
11 regulation.

12 That pales in comparison to the 3 million
13 that companies have to spend to comply with GDPR.

14 Another important lesson learned from GDPR is
15 that it provides for a national standard.

16 The EU has one continent-wide standard that
17 recognizes for the cross-border data flows.

18 This is an important goal, and one that the
19 United States should also be considering.

20 In -- individual state laws could result in
21 the fragmented Internet while providing consumers
22 with different online experiences.

23 Consumers in New York should be provided with
24 the same online experiences as their -- as a
25 resident in other states, such as California or

1 Florida or Washington.

2 I think that those are -- should be helpful
3 in informing the discussion, but I would also like
4 to briefly touch on two of the bills before the
5 Legislature this year.

6 TechNET is strongly supportive of the
7 SHIELD Act. We believe it is the most reasonable
8 and balanced approach to updating the data-breach
9 laws here in New York.

10 In my written testimony, we have offered some
11 suggested improvements to that legislation.

12 TechNET is also strongly opposed to the
13 New York Privacy Act, as written.

14 As I mentioned, these are very important
15 topics that require a lot of thought and
16 deliberation.

17 And the tech community would like to continue
18 to work with the Legislature on those topics in the
19 future.

20 Thank you.

21 TED POTRIKUS: Good morning, Chairs Thomas
22 and Savino, Senator Liu.

23 My name is Ted Potrikus, and I'm president
24 and CEO of the Retail Council of New York State here
25 in Albany.

1 Thank you for the opportunity to be here.

2 We all shop.

3 We all know that, when you get online,
4 somebody is watching, and we're all trying to figure
5 out what you want as customers.

6 What retailers, large and small, have learned
7 over time is that customers, generally, will be
8 happy to share an e-mail address, first and last
9 name, and/or a mailing address in exchange for
10 instant discounts, coupons, reduced or free
11 shipping, or other types of loyalty programs, such
12 as VIP points, airline miles, and the like.

13 Fewer are willing to share a phone number for
14 calling or texting, realtime location data, or
15 allowing offers from other merchants.

16 Fewer still, very few we found, are eager to
17 share information like a social-media account,
18 credit card numbers, driver's license number, or
19 biometric data, regardless of the size of the
20 benefit that they might receive.

21 We also know that shoppers will walk.

22 If a retailer mishandles or misuses the data
23 the customers have given freely, they'll lose the
24 business.

25 In short, retailers use consumer data for the

1 principal purpose of serving their customers as they
2 wish to be served.

3 Retailors' use of personal information is not
4 an end in itself, but, primarily, a means to achieve
5 the goal of improved customer service.

6 This differentiates retailors' principal use
7 of data from businesses, including service
8 providers, data brokers, and other third parties,
9 unknown to the consumer, whose principal business is
10 to monetize consumer data by collecting, processing,
11 and selling it to other parties as a
12 business-to-business service.

13 Such data practices are the profit center of
14 the big data industries, whose products are the
15 consumers themselves rather than the goods sold to
16 consumers.

17 As you consider privacy legislation, we hope
18 you will recognize the fundamental differences in
19 consumer-data usage between two categories of
20 business:

21 First-party businesses, such as retailors,
22 which sell goods or services directly to consumers,
23 and use their data to facilitate sales, provide
24 personalization, recommendations, and customer
25 service;

1 And third-party businesses, which process and
2 traffic in consumers' personal data, very often
3 without consumers' knowledge of who is handling
4 their data, and for what purpose.

5 The FTC, in 2009, explained in a staff report
6 on online advertising, the distinct differences they
7 found between first- and third-party uses of data,
8 particularly regarding consumers' reasonable
9 expectations, their understanding of why they
10 receive certain advertising, and their ability to
11 register concerns with or avoid the practice.

12 The FTC basically said, that the consumer is
13 likely to understand why he or she receives targeted
14 recommendations or advertising in the case of
15 first-party sharing, but not in the case of third.

16 Given the global nature of the topic at hand
17 and the inescapable truth of jurisdictional limits,
18 the Retail Council agrees, fundamentally, that
19 matters of consumer privacy are best addressed at
20 the federal level.

21 We also acknowledge that Congress does not
22 always move at a pace acceptable to New York State;
23 and, therefore, recognize the appropriateness of
24 your hearing today and the bills your committees
25 consider on the matter of consumer privacy.

1 With that in mind, we offer a few general
2 principles we believe are essential to any
3 discussion on potential legislation.

4 Among them:

5 The preservation of consumer awards and
6 benefits that we all want;

7 Maintain transparency in consumer choice;

8 Industry neutrality;

9 Data security of breach notification at the
10 strongest level.

11 As for the legislation currently before the
12 state Legislature, we'll jump right into the pool
13 with our colleagues here at the table.

14 The SHIELD Act, the attorney general's office
15 has been great working with us over the past few
16 years on coming up with something, and that's a good
17 bill.

18 We are very concerned about the New York
19 Privacy Act that has just come in, for the reasons
20 that were expressed here.

21 And, notwithstanding our opposition as it's
22 currently drafted, we appreciate the opportunity to
23 work with you.

24 And I know that the retailers that are
25 members of the council will be happy to work

1 constructively with you on that, and any other
2 legislation, going forward.

3 So, thank you for the time today.

4 SENATOR SAVINO: So --

5 OFF-CAMERA SPEAKER: Two-minute balance.

6 SENATOR SAVINO: Huh?

7 OFF-CAMERA SPEAKER: Good job. Two minutes'
8 balance.

9 SENATOR SAVINO: Excellent.

10 So thank you all.

11 SENATOR THOMAS: You could talk for two more
12 minutes -- no.

13 SENATOR SAVINO: Thank you all for your
14 testimony.

15 Halfway through I said to Senator Thomas,
16 I said, I'm noticing a theme.

17 We like the SHIELD Act. We don't like the
18 Data Privacy Act.

19 So I just have a question for all four of
20 you, because I -- in listening to you, you talked
21 about the difficulty of complying with the Data
22 Privacy Act -- with the New York Privacy Act; the
23 compliance problems that would exist, the costs
24 associated, the burden it would place on businesses.

25 But the question I have is:

1 Isn't it true that, in 2017, after the
2 department of financial services, working with
3 industry professionals and others, released new
4 rules on February 16th; after two rounds of feedback
5 from industry and the public, instituted regulations
6 around the ever-growing threat posed to financial
7 systems by cybercriminals?

8 And now we are design -- they were designed
9 to ensure businesses effectively protect their
10 customers' confidential information from cyber
11 attacks, including conducting regular security-risk
12 assessments, keeping audit trails of asset use,
13 providing defensive infrastructures, maintaining
14 policies and procedures for cybersecurity, and
15 creating an incident-response plan.

16 And all of those requirements are in place
17 for people who do business with the State and/or
18 including, but not limited to, State-chartered
19 banks, licensed lenders, private lenders, foreign
20 banks licensed to operate in New York State,
21 mortgage companies, insurance companies, service
22 providers.

23 So I think the question I'm saying is: All
24 of those entities could figure out how to do what,
25 essentially, is included in the New York Privacy

1 Act, why couldn't everybody do that?

2 Most of what Senator Thomas wants to do, as
3 I understand it, is enshrined in the regs that were
4 adopted by DFS for these institutions, because of
5 the concerns about cybersecurity and data breaches,
6 and the protection of people's information.

7 How much bigger would the burden be for
8 everybody else, if they've already figured it out
9 for those institutions, if you can answer that?

10 ZACHARY HECHT: So I think one of the
11 distinctions here is between data security and data
12 privacy.

13 The cybersecurity regulations, I'm less
14 familiar with them, but, as I understand them,
15 companies are responsible for putting plans into
16 place for protecting cybersecurity. And they were
17 given some latitude with how those plans would look;
18 there were specific requirements.

19 And I think that mirrors closely to what the
20 SHIELD Act is doing, to some extent, and there is
21 the notification of the attorney general.

22 But the data privacy -- the New York Privacy
23 Act is distinct, and it would require companies to
24 rework database systems, it would require them to
25 rework internal processes, that could conflict with

1 their business models. And it gives less latitude
2 to the companies, and it's a bit different in scope
3 than the security regulations.

4 SENATOR SAVINO: So -- maybe -- so is there a
5 difference between protecting customers'
6 confidential information and protecting their data?

7 JOHN OLSEN: Well, I think --

8 SENATOR SAVINO: And that's an actual --
9 I mean, I don't know the answer to that.

10 JOHN OLSEN: -- yeah, no, you have a pretty
11 good point.

12 What I would point out, though, is, in the
13 Data Privacy Act, there is a provision that allows
14 for the private right of action, which is not found
15 in DF (sic) regs.

16 When you combine that with certain
17 definitions, including "personal data," "privacy
18 risk," and "opt-in," which is affirmative consent to
19 the use of processing, collection, and sale of data,
20 and then you empower the, you know, regular
21 Joe Public to then go after a company that does not,
22 you know, consider their privacy risk and their
23 fiduciary duties, I think what you're running into
24 is a lot of problematic litigation, in the interest
25 of trying to decide whether or not, you know, that

1 person has a legitimate case or not.

2 When you enshrine in state law these kinds of
3 provisions, you're running the risk of giving a lot
4 of, you know, individual residents the power to
5 financially hurt companies.

6 With the DFS regs, this is a State entity
7 that is taking the step to require businesses to
8 update their cybersecurity measures, and to have, at
9 least at, you know, some level, a floor for the
10 protection of sensitive data.

11 This, essentially, would empower the
12 residents to determine what is a, you know, positive
13 user experience when dealing with specific websites
14 or companies that handle their personal data.

15 SENATOR SAVINO: And, certainly, a private
16 right of action is a weapon, I understand that.

17 But, the violations that DFS has put in place
18 for the fines, as a result of violations, are pretty
19 steep too.

20 So, up to \$250,000, or, up to 1 percent of
21 total banking assets. So it's not insignificant
22 there either.

23 But I hear your point on it.

24 At this point I'll hand it over to
25 Senator Thomas.

1 Thank you.

2 SENATOR THOMAS: All right. I believe
3 Senator Liu has a couple of questions.

4 SENATOR LIU: (Microphone turned off.)

5 Thank you, Mr. Chair.

6 I want to say from the outset that,
7 unfortunately, as you know, we have a lot of --

8 (Microphone turned on.)

9 Thank you, Mr. Chair.

10 I want to say from the outset that, as you
11 know, we have lots of things going on today, so
12 I will probably have to leave after this panel and
13 head over to the other meeting.

14 But I do appreciate this panel's input.

15 I support Senator Thomas's bill, the privacy
16 bill.

17 I understand, I think the main argument is,
18 that you feel this kind of regulation is more
19 appropriate at the federal level.

20 But as Mr. Potrikus mentioned, Congress is
21 sometimes slow to act. So sometimes states,
22 especially -- we like to think, especially the State
23 of New York, acts before, and perhaps gets Congress
24 to move a little quicker, and maybe they'll adopt
25 many of the provisions that we envision here in

1 New York.

2 So my quick question to you, and I'm asking
3 for a succinct answer, is, if Senator Thomas's bill
4 were to be enacted at the federal level:

5 What would be -- what -- would you have
6 serious misgivings about such a bill at the federal
7 level?

8 Or, would you largely think it's in the right
9 direction, maybe some tweaks here and there?

10 TED POTRIKUS: I will start with that.

11 I think we would oppose it at the federal
12 level as well.

13 One of the concepts that was brought up was
14 that, the new definition of "data fiduciary," which
15 in the couple of weeks that we've had to take a look
16 at this -- at this bill, I know that that's raised a
17 lot of alarm within the retail industry, as to what
18 that ultimately means, and the level of liability
19 that that puts in front of retailers, particularly
20 when it's combined with the private right of action
21 that was brought up.

22 So I think, as currently drafted, the answer
23 to that would be, yes, we'd have similar concerns at
24 the federal level.

25 SENATOR LIU: Okay. I mean, just to be

1 clear, please don't say "as it's currently drafted,"
2 because, obviously, you know, no bill goes from its
3 original draft form to passage unscathed.

4 So my question was: Largely speaking, are we
5 on the right track with this legislation?

6 Maybe some tweaks need to be made here and
7 there?

8 Or are there more than tweaks that need to be
9 made in order for this to make sense federally --
10 nationally?

11 Are there significant chunks that need to be
12 overhauled, or eliminated, or other things that
13 we're missing, that should be implemented as part of
14 a national law?

15 JOHN OLSEN: Succinctly, yes.

16 There is --

17 SENATOR LIU: "Yes," what, just to be clear?

18 JOHN OLSEN: Yes, we have to take out quite a
19 bit of this bill.

20 With all due respect to the Senator, this
21 bill is unworkable.

22 What we're seeing with GDPR, which a lot of
23 this is borrowed from, is significant compliance
24 issues and great cost.

25 Americans need an American privacy law.

1 This borrows from a European model that
2 was you know, first conceived and vetted over
3 four years, and then debated for another four years,
4 before it went into implementation.

5 After one year, GDPR is, in some respects,
6 effective, but is very compliance-heavy.

7 The attempt in California with the CCPA has
8 good concepts, but needs a lot of work, still, in
9 the current legislative process before it can be a
10 workable model as well.

11 So, in respect to the Privacy Act here in
12 New York, to apply it at the federal level, would
13 almost exponentially increase all the problems that
14 we would see in New York.

15 I think what you'd have is significant
16 compliance concerns.

17 And, also, you know, generally, the concept
18 of data fiduciary, you know, coupled with privacy
19 risk, is going to fundamentally alter a user
20 experience.

21 We could have it at the state level or we
22 could have it at the national level.

23 But what we're seeing with GDPR is,
24 noncompliance sites just don't show up in search
25 results. Or, you have notices that are, you know,

1 basically mandated for every website you visit, that
2 says, Do you want your information shared?

3 It's an opt-out in the European concept.

4 This concept, it's an opt-in; it's an
5 affirmative consent.

6 And you're -- if you do not consent, you're,
7 under this bill, not obligated to having altered
8 user experience, but, that is open to
9 interpretation.

10 So if you were to implement this bill with
11 the private right of action, you're, essentially,
12 empowering anyone in the United States to then say,
13 My experience with, you know, Company A has been not
14 to my satisfaction, so I am going to seek legal
15 action.

16 SENATOR LIU: Thank you, Mr. Olsen.

17 How about the other two experts?

18 ZACHARY HECHT: So I think if it was a
19 federal bill, it also would be very problematic.

20 And still going beyond the compliance costs,
21 I think we can understand that it is very costly,
22 and that is something we are very concerned about.

23 But going beyond that, there are significant
24 First Amendment concerns with the parts of the bill
25 that are taken from GDPR.

1 There's a different constitutional framework
2 there. And if you bring some of that over here,
3 you'll have free-speech and free-expression
4 concerns.

5 And if you look at the "data fiduciary"
6 concept, which is relatively new, it's been written
7 about quite a lot in the -- you know, in academia,
8 the "data fiduciary" concept looks to address the
9 First Amendment concerns of GDPR and sort of be an
10 alternative.

11 So, here, you're taking the data fiduciary
12 and you're putting it alongside the things that are
13 recognized First Amendment concerns about.

14 And then the way that the data fiduciary is
15 set up here, there would be concerns because
16 publicly-traded companies have a fiduciary duty to
17 their shareholders.

18 So, would this new fiduciary responsible
19 supersede that? How would those work together?

20 And then the way that the data fiduciary is
21 described here is quite broad.

22 A lot of the legal work that talks about data
23 fiduciary says that it's a very -- in certain
24 context, it needs to be narrowly framed.

25 And this is very broad.

1 So I think if it was federal, that would be
2 the First Amendment concerns and free-speech
3 concerns.

4 CHRISTINA FISHER: We would also be opposed
5 to it at the federal level, for many of the same
6 reason that my colleagues here have already
7 expressed.

8 We have very serious concerns with the
9 fiduciary concept in a private right of action.

10 So, at a federal level, it would be serious
11 work.

12 SENATOR LIU: Okay.

13 Well, thank -- Mr. Chairman, thank you.

14 I appreciate the responses from these
15 individuals.

16 I know that the Chairman and his staff
17 convened this hearing, and put together the panels.

18 My -- my impression from this panel is that
19 you mostly represent industry and business.

20 And there's a lot of emphasis on the cost to
21 the businesses, to the corporations, which, of
22 course, we have to consider.

23 But on the other hand, and I suspect we'll
24 hear from other people a little bit later, from a
25 consumer point of view, there's been a lot of

1 information taken from consumers, a lot of loss of
2 privacy.

3 And business and the corporate sector has
4 profited significantly from that consumer
5 information.

6 So, any kind of regulation that seeks to
7 protect consumers will impose some kind of cost on
8 business.

9 So to say that, you know, it's going to be a
10 minimal cost if we impose some kind of a regulatory
11 regime, whether it be at the state level or the
12 federal level, that -- that's a given, because we're
13 trying to protect consumers.

14 And that's always going to require businesses
15 and the corporate sector to give up some of their
16 huge profits that they've already been getting for
17 many years at this point.

18 So I just want to, hopefully, help frame the
19 discussion there.

20 But I appreciate your input, and I know we
21 look forward to working with you.

22 SENATOR THOMAS: All right, my turn.

23 So just like Senator Liu and Senator Savino
24 said, I mean, the two bills that are in the
25 Legislature right now about privacy, one being the

1 SHIELD Act, and one being the New York Privacy Act,
2 both are my bills.

3 And you like one, and not the other.

4 So I, technically, win, because you guys like
5 at least one.

6 All right, so getting to the New York Privacy
7 Act, right, so how would you define "personal data"?

8 JOHN OLSEN: That's a bit of a loaded
9 question.

10 I would start with the less broader
11 definition. You know, I don't want to get into
12 detail about what would constitute an appropriate
13 definition.

14 I mean, what we've seen in other states, you
15 know, other state attempts, what we're seeing in --
16 with the California law, is there definitely needs
17 to be consideration for certain components,
18 especially when it comes to things like Internet
19 protocol address, or something like that.

20 You know, there's some significant concerns
21 with, when you use that as a marker, what exactly
22 are you giving, you know, the ability to, like a
23 household, say?

24 Because "a household" doesn't necessarily
25 just mean a family. It could mean roommates, or

1 perfect strangers, that are sharing one modem.

2 So your Internet protocol address is,
3 essentially, tied to that modem. And now you're
4 empowering certain people to have access to your
5 personal information; or to say, you know, because
6 their personal experience, based on that set of
7 personal data, was different, now, you know,
8 whatever company was providing a service is under
9 the gun to explain whether or not they believe they
10 were in violation of the fiduciary duty.

11 So I think there's a concern there with
12 certain definitions.

13 TED POTRIKUS: And I think, from the
14 retailers' perspective, and, Senator Liu, you
15 pointed out, you know, the need to look at this from
16 a consumer perspective, and how the shopper, in our
17 case, would define "personal information," just
18 thinking about what we found over the years, working
19 with, and getting information from, the people who
20 shop in our stores, or on our websites, it's what
21 they're willing -- what they're willing to share
22 with us.

23 And I mentioned that briefly in our
24 testimony, and it's in our written testimony, about
25 the level of comfort that a shopper generally has.

1 You know, they'll share name, mailing address,
2 sometimes the e-mail address.

3 The farther you go on the ramp toward more
4 granular personal data, the less willing the
5 consumer seems to be to share that regardless of
6 what benefit they get.

7 I think -- I think sometimes this has to be
8 looked at as a balance: What's "personal
9 information," and what are we as consumers willing
10 to give; and in exchange, what do we get?

11 Again, just speaking on the retail-industry
12 side:

13 Do you get VIP points?

14 Do you get discounts?

15 Do you get reduced or free shipping?

16 Do you get speedier shipping?

17 What's -- what's on the other side of that
18 equation for the shopper?

19 And I think, as we, as an industry, try to
20 figure out what "personal data" means, and "personal
21 information," it's, how do you strike that balance
22 with your shopper? that we find.

23 SENATOR THOMAS: The other two experts, any
24 comments?

25 CHRISTINA FISHER: I would not be able to

1 offer a definition for you today, but I would like
2 to continue to offer the opportunity to continue to
3 work with you.

4 I think something worth noting, is that this
5 bill has a lot of really complex topics.

6 And I think there's a lot that needs to be
7 digested, and a lot more conversations that needs to
8 be had around this topic.

9 And I think the technology community is more
10 than willing to be at the table, continue to have
11 those conversations.

12 And I think that there is a balance that can
13 be struck between protecting consumer privacy while
14 also allowing consumers to be able to enjoy the
15 online experiences that they expect from companies.

16 ZACHARY HECHT: Echoing what my fellow
17 panelists said, and then also just keeping in mind
18 that there needs to, at some point, be harmonization
19 between the definitions that exist internationally.

20 So you have to look at what happened in
21 Europe. And anything in the United States has to
22 look a little bit like that, even if there's some
23 tweaks.

24 It makes sense for compliance.

25 SENATOR THOMAS: From reading the New York

1 Privacy Act, do you believe that my definition of
2 what "personal data," is it too broad? is it too
3 narrow?

4 Do you have a comment on that?

5 TED POTRIKUS: I'll officially punt.

6 I'll get back to you on that one.

7 SENATOR THOMAS: All right.

8 All right, I'll go to the next question.

9 Since we talked a lot about GDPR, GDPR relies
10 on opt-in consent, where users have to explicitly
11 choose to share data, while bills in the
12 United States generally allow for opt-out consent,
13 where users have to explicitly withdraw consent.

14 Why is opt-in consent, that makes it easier
15 for the consumer to make an informed choice about
16 the data, not a better approach?

17 JOHN OLSEN: I don't think it's, you know,
18 not a better approach.

19 I think what you're combining it with is the
20 problem.

21 You know, the affirmative consent for the
22 collection, processing, or sale of data is where we
23 get into the issues of, just what is a company
24 allowed to get from a consumer to operate their
25 business model?

1 It's not simply about cost.

2 It's really about how the platform functions.

3 You know, in respect to certain services that
4 are provided to consumers for free -- search
5 engines, mapping, geolocation services, things like
6 that -- you know, certain data needs to be
7 exchanged.

8 And if a person just says, I'm opting in or
9 I'm opting out, how they determine whether they want
10 those services or not could be subject to what
11 they're opting in or opting out of as far as
12 personal data.

13 The definitions matter when you talk about,
14 what -- you know, what is a reasonable expectation
15 for a user when they access a website?

16 If they're not affirmatively consenting, then
17 no information is even collected.

18 So how do you make a determination about how
19 to best tailor services to that individual if
20 they're not opting in to your business?

21 TED POTRIKUS: I would agree with everything
22 that John just said.

23 Simply, the consumer experience that people
24 expect when they go to a retailer's website, you
25 know, I think we're all trained now to get

1 recommendations based on things that we've looked at
2 before, or, you get coupons based on things that
3 you've purchased before.

4 And that's the sort of information that
5 I think John is talking about with protecting, the
6 opportunity to still have that.

7 And, if we had to make changes to the
8 website, you could be upending that entire process.

9 And I think it leaves customers a little bit
10 in the lurch, not knowing what they've said yes to,
11 what they've said no to.

12 ZACHARY HECHT: So -- and as you heard, so
13 opt-in has -- creates some concerns around the
14 delivery of the service.

15 But beyond that, what are we actually getting
16 at with opt-in?

17 If you go to Europe right now, and there's
18 the opt-in framework, you go, and there's a little
19 notice in the bottom of your screen. You flick it
20 away, you hit "yes," and that's what "opt-in" is.

21 There are some other frameworks that it could
22 be, you know, put forward in.

23 But, if that's what we're going for, and then
24 there are all the concerns with, is that really the
25 best way forward for consumer privacy?

1 SENATOR THOMAS: So based off of what all
2 four of you have just said, it's just a matter of
3 the user experience; right?

4 Opting in kind of changes the entire website
5 experience, et cetera.

6 That's what we're coming at here, if we opt
7 in versus opting out.

8 Right?

9 Okay.

10 All right, next question: Given how personal
11 information is like gold today, should a company
12 benefit from consumers' data to the detriment of a
13 consumer?

14 It's a yes or no.

15 ZACHARY HECHT: I mean, what's "the
16 detriment" of the consumer? So what are we defining
17 that as?

18 I know in the bill you establish "privacy
19 risk" as a set of things.

20 But it's --

21 SENATOR THOMAS: For example, financial loss
22 to a user, embarrassment, or fear.

23 JOHN OLSEN: I actually want to explore that
24 concept of embarrassment.

25 Can you expound on that a little bit, when

1 you're talking about privacy risk?

2 There's some curious definitions with privacy
3 risk.

4 The "physical harm," "psychological harm,"
5 that, you know, I get that, loss of finances.

6 The "embarrassment or altered experience,"
7 I'm a little confused.

8 So I just -- where you were going with that,
9 I'm curious.

10 SENATOR THOMAS: Just in terms of, like,
11 photographs.

12 Like Facebook, for example, yes, they have
13 these privacy protocols.

14 But what if another party, another partner of
15 theirs, uses it to the detriment of the user?

16 Kind of manipulating them in a way.

17 Kind of figuring out what their emotions are,
18 and then targeting them with ads.

19 That's what I'm kind of getting at here.

20 JOHN OLSEN: Okay.

21 I mean, it's a strange approach.

22 I think what we really need to do is to have
23 a lot more stakeholder input about what is impactful
24 to a consumer.

25 Also, what is a consumer willing to give up

1 if they're no longer allowed to use these services
2 as they normally did?

3 You know, the exchange of personal
4 information, personal data, is the relationship with
5 these companies.

6 There was a study done by "The Economist"
7 that essentially said, you know, if you were to be
8 paid for the services that you were receiving for
9 free, to not use them anymore, what is the actual
10 value?

11 And for search engines, it was in the tens of
12 thousands of dollars. For mapping services, it was
13 in the thousands of dollars.

14 So you're talking about a lot of value
15 provided to a consumer for the exchange of personal
16 information.

17 When you talk about privacy risk with that
18 personal information, be it a photograph or not,
19 I think you're asking companies to really speculate
20 on individual emotion, and, you know, just their
21 general outlook.

22 And I think the biggest issue is, whether we
23 want this litigated in the courts when it comes to
24 the private right of action, where I said:
25 I suffered embarrassment. This company owes me

1 money.

2 And now you leave it up to a judge to say,
3 well, yeah, you have a case here, or, no, you don't.

4 You know, I think that's the real concern
5 when you empower people through these definitions,
6 and then provision of private right of action, to
7 then say, I've suffered embarrassment.

8 I mean, where is the line drawn as far as
9 what the company's liability is?

10 That's, I think, what we need to continue the
11 conversation about.

12 SENATOR THOMAS: That doesn't really answer
13 my question, but (indiscernible cross-talking).

14 ZACHARY HECHT: So I think that we will say
15 that, we need to be in a place where the use of data
16 does not go to the detriment of the consumer when
17 the "detriment" is defined as some of these clearly
18 delineated legal, you know, definitions we've had.

19 So, financial harm, there are already some
20 protections in place.

21 There are some federal data-protection
22 frameworks that protect financial information.

23 And things of that nature are important, and
24 companies should not be using data to the detriment
25 of those.

1 But when you get to some of the other
2 definitions, I think, you know, "inconvenience of
3 time," some of the -- you know, you have, "alters
4 individual's experiences," that's less clear what
5 we're talking about there.

6 And if we're talking about the deliverance of
7 ads and things of that nature, there are free-speech
8 concerns and commercial-speech concerns there.

9 And we have to be very careful with how we go
10 through those definitions.

11 TED POTRIKUS: I think I would just add that,
12 as you're looking at this with some subjective
13 concepts, it's -- that's where we start to get into
14 the thing that we were referring to in our written
15 testimony about the first-party users and the
16 third-party users.

17 I do know, in the case of a first-party user,
18 all it takes is one misstep and they've lost the
19 customer.

20 So I think, as far as, to your question, you
21 know, the financial harm, there are standards for
22 that.

23 Some -- somewhere there are no specific
24 definitions. And trying to put a subjective concept
25 into an objective set of rules I think is the

1 challenge.

2 SENATOR THOMAS: Okay.

3 I just want to move on to the next question.

4 There have been countless instances where
5 companies exposed private information to third
6 parties, and decided not to disclose it to the
7 public.

8 Should a state law establish that there be
9 disclosure once a breach occurs?

10 JOHN OLSEN: Yeah, I think that's the
11 SHIELD Act.

12 That's why this is the commonsense approach
13 to addressing a real issue when it comes to consumer
14 data and private information.

15 If there is a breach, then there should be,
16 you know, a significant disclosure in a timely
17 manner.

18 So that's why we support the SHIELD Act.

19 SENATOR THOMAS: Anyone else?

20 Same thing?

21 ZACHARY HECHT: Agreed.

22 SENATOR THOMAS: Okay.

23 Should disclosure be limited to situations
24 where there is measurable harm?

25 TED POTRIKUS: I think if -- I'm not an

1 expert here, but I'll take a shot at it, just from a
2 consumer standpoint, almost.

3 I think the key is, making sure that the
4 notice is for a reason, because, you know, every
5 year you get those things that says, This is not a
6 bill, or, This is just our annual privacy notice.

7 I'm not sure that people read them anymore.
8 It's like too many signs on the road.

9 And if you start to get a notice every time
10 there is a breach of, you know, is it one?

11 Does -- does one set of data/does one
12 person's data constitute a breach? you know, I think
13 you get into the situation where the impact of the
14 notice is diminished.

15 So I think there -- it has to be for a reason
16 in order for it to be effective, and to really -- to
17 make sure that the consumers pay attention to it in
18 a way that we would want them to.

19 SENATOR THOMAS: What are the reasons a
20 company needs to hold on to information for extended
21 periods of time?

22 ZACHARY HECHT: It depends on the context
23 that we're talking about, and what kind of
24 information.

25 If it's financial information, and you are an

1 e-commerce platform, it might be so that customer
2 can come back and, once again, go through your
3 system; or, it's held in a separate place in an
4 encrypted manner.

5 But it depends on the context that we're
6 talking about.

7 JOHN OLSEN: I think legal obligations,
8 ongoing litigation, or anything like that, and there
9 are certain retention periods that are standard
10 policy.

11 I think, for the most part, you know, many
12 companies just retain information in case of
13 litigation.

14 SENATOR THOMAS: Is there a standard holding
15 time for personal data, for example, that is, you
16 know, used industry-wide?

17 JOHN OLSEN: Not uniformly.

18 SENATOR THOMAS: No, not uniformly.

19 JOHN OLSEN: I think it would be company to
20 company.

21 SENATOR THOMAS: Is there an average time
22 they hold the information for?

23 TED POTRIKUS: I'm not sure that there would
24 be. You know, it is going to vary from company to
25 company.

1 But it comes down to the -- if we go back, we
2 talked about this this morning, with the customer
3 experience on the website.

4 And, again, let's talk about a retailer
5 website.

6 You know, do you want to enter your password?

7 Do you want to put in your credit card
8 number?

9 How much do you want to enter each time?

10 And I think that that's up to the individual
11 customer.

12 But I think as long as you're -- as long as
13 you're going back to that website, or visiting it,
14 buying from it, using it, that's how long they'll
15 keep the information.

16 SENATOR THOMAS: Would you say, like, holding
17 that data for a long time leaves a company to a
18 breach?

19 For example, let's say you're shopping on
20 Amazon, and, I get it, you know, you're storing that
21 credit card information on Amazon.

22 And, should there be a time limit in which
23 Amazon says, All right, we're going to keep this
24 information for, like, six months, for example, and
25 then you have to reenter it in order to purchase

1 again; this a way, avoiding a security breach, for
2 example?

3 You know, because, what hackers want are
4 those credit card information, the names, the
5 addresses.

6 So holding it for a long time would open them
7 up to a breach, in a way, because they know that
8 there's gold there.

9 Do you think holding it for a short period of
10 time, and then asking the user, "hey, enter this
11 information again because your information has
12 expired," would kind of enhance the security?

13 ZACHARY HECHT: I'm not sure.

14 I don't think it would.

15 So if a company is holding on to it for a
16 specific amount of time already, I'm not sure that
17 then deleting, and having the customer simply
18 reenter it as soon as they go back, lessens the
19 target.

20 And companies are keeping it in a secure --
21 generally, and, according to some of the laws that
22 we are talking about today, they keep it in secure
23 databases and in secure systems.

24 So if a customer is then submitting that
25 information again, it opens up for increased risk,

1 potentially.

2 SENATOR THOMAS: Okay.

3 We're seeing children's privacy being
4 violated.

5 You know, a lot of kids use Facebook, they
6 use Instagram.

7 And, recently, there was news about,
8 I believe, the Amazon device listening in to
9 children's conversations, and parents trying to
10 delete it, but they couldn't be deleted.

11 Should there be a right to delete?

12 JOHN OLSEN: I think the right to delete is
13 more of a European concept.

14 You know, as Zach has alluded to previously,
15 there is some First Amendment issues when you talk
16 about the right of deletion.

17 I can speak for a lot of my members, that
18 there are already policies for the deletion of data
19 upon request.

20 To mandate in state law, I think runs into
21 certain First Amendment issues, to the point about,
22 you know, children's privacy.

23 I and my members strongly support legislation
24 regulation that, you know, strictly enforces the
25 ability for children to be protected.

1 But we cannot, you know, mandate certain
2 things that run afoul of American values and
3 concepts.

4 SENATOR THOMAS: Should there be even greater
5 privacy for those under 18 years of age?

6 JOHN OLSEN: I don't know what "greater
7 privacy" means.

8 I think we, again, need to all be at the
9 table to talk about what these concepts, and, you
10 know, at what levels are appropriate, especially in
11 the state level.

12 ZACHARY HECHT: So I think the specific age,
13 there's some conversation over it.

14 But I -- there's already a federal framework.
15 It's called "The Children's Online Protection
16 Privacy Act." And that applies to children under
17 the age of 13.

18 So there's already a higher standard there.

19 And if we're talking about some of the
20 incidents you were talking about on some the
21 devices, I think we also need to look to where the
22 tech ecosystem is moving, and where companies are
23 moving. And those are things like federated
24 learning.

25 So that would be, in the case of the

1 listening device that you talked about, or the home
2 assistant, where there would be no actual data
3 sharing. It would just be locally.

4 And that it would then pull insights, and
5 then go to the company. But there would be no
6 personally identifiable information shared.

7 You've got things like differential privacy,
8 where there is noise added to the data.

9 And we see a lot of the tech industry moving
10 there at this point.

11 So we need to also keep those in mind when
12 we're legislating this space.

13 SENATOR THOMAS: Let's go into targeted
14 advertising.

15 Can someone explain to me how an online
16 company targets users with ads?

17 TED POTRIKUS: I think in the case of the
18 retailers specifically, and I'll go back to what we
19 referred to in our testimony, the first-party users
20 and the third-party users, the first-party users/the
21 retailers will take your browsing, your buying, and
22 that's where you start to see, you know, the
23 advertising when you get back, or the e-mail that
24 you get back, from the place that you just shopped,
25 that, suddenly, you know, even though you just spent

1 a few hundred dollars on the website, please come
2 and spend more, we have more coupons for you.

3 But this is how they do it: They take your
4 experience, and they get right back in touch with
5 you.

6 I think what differentiates, in large part,
7 that first party versus the third, is the ability to
8 directly contact the retailer and say, knock it off.

9 You know, where you can go back to the store
10 that you were just working with, and saying:

11 I don't want this.

12 Or, keep it coming, I do want this. I want
13 more coupons. I want more advertisements, to let me
14 know when lawn furniture is going to go on sale, or
15 winter jackets are going to go on sale.

16 So I think that puts a lot of the control, in
17 that case, in the hands of the consumer.

18 How an ad shows up on "The New York Post"
19 website, when I was walking down the street,
20 thinking about a bicycle. And I turn on my computer
21 and I see an ad for a bicycle, I'm not quite sure.

22 SENATOR THOMAS: Anyone else?

23 ZACHARY HECHT: I think it's important to
24 keep in mind that there are different models of
25 serving ads.

1 There are contextual advertisements, which
2 are not based necessarily on your individual
3 demographic.

4 And then there are other personal ad
5 services.

6 But there is a variety of models out there.

7 SENATOR THOMAS: Okay.

8 In your -- in all of your testimony, you
9 talked about how the data fiduciary has not been
10 used anywhere.

11 But there is a federal law -- I mean, a
12 federal bill, actually, the Data Care Act, which was
13 introduced in 2018, that talks just about, you know,
14 this duty of loyalty, whereby you think of the user
15 versus, you know, the profit-making schemes of the
16 company.

17 You talk about how, you know, we should look
18 to the federal government to push forward with
19 privacy, because, to try to comply with every
20 state's different privacy rules would be very
21 complicated and difficult.

22 Do you believe if -- in the federal
23 government, if they were to enact a data fiduciary,
24 would you agree with it then?

25 ZACHARY HECHT: So just to echo what I said

1 before, the fiduciary concept has conflicts with the
2 fiduciary duty to the shareholder.

3 And then beyond that, I think the federal
4 bill is much more narrowly defined than your
5 Privacy Act.

6 So that's something to also keep in mind.

7 JOHN OLSEN: Yeah, I am supportive of
8 Senator Schatz's bill because of its narrow scope,
9 and because it does not, you know, require certain
10 things, like, fiduciary duties to shareholders being
11 superseded by, you know, consideration of privacy
12 risks to New York residents, or, in the case of a
13 federal law, United States residents.

14 So I think if we're talking about data
15 fiduciary as a concept, the more narrow and focused
16 it is, the more supportive we would be.

17 SENATOR THOMAS: All right.

18 I heard a lot about the negatives of the
19 New York Privacy Act.

20 Do you like anything about my bill?

21 [Laughter.]

22 OFF-CAMERA SPEAKER: Say "the sponsor."

23 ZACHARY HECHT: The sponsor.

24 SENATOR THOMAS: Oh, thank you, Zach.

25 You're my favorite now.

1 JOHN OLSEN: No, I think there are some
2 concepts that are workable.

3 You know, it's, the devil is in the details.
4 And it's a common phrase, but it really does
5 mean a lot when it comes to privacy law.

6 This is a very complex issue, and, you know,
7 we welcome the opportunity to be talking with you.

8 I am here to provide insight and guidance,
9 but we need to, you know, think about what language
10 is actually put in a bill.

11 I mean, we need to work, you know, more
12 closely.

13 SENATOR THOMAS: So you're basically saying,
14 if we narrow the definitions down, and, basically,
15 you know, narrow the "data fiduciary" definition as
16 well, this would be a workable bill?

17 JOHN OLSEN: I think if you take out private
18 right of action; if get more specific on, you know,
19 the harm or privacy risk; and you really, you know,
20 bear down on what exactly you're, you know,
21 requiring New York businesses to comply with, then
22 we could have the start of a conceptual bill.

23 SENATOR THOMAS: Anyone else?

24 TED POTRIKUS: No, I would say that, that
25 what we like about it is the fact that you're taking

1 the time today to have this hearing, and to include
2 us at the table, and to not just move forward with
3 something, and you're taking this time to listen to
4 us, and to listen to everybody else who will be on
5 the panels today.

6 You know, without that, then we can't go with
7 you to that public-policy goal that you've
8 established.

9 Because you've brought us here now, you know,
10 like everyone here has said, we're happy to be here,
11 and we'll work with you on it as you try to get to
12 this point that you want to get to with your goal
13 for the public policy.

14 SENATOR THOMAS: Thank you all.

15 Any questions?

16 All right.

17 Panel one is dismissed.

18 ZACHARY HECHT: Thank you.

19 SENATOR THOMAS: All right, the second panel
20 has assembled.

21 Again, I would like to apologize if
22 I slaughter anyone's name. It doesn't look like
23 complicated names, but if I do, I apologize.

24 So Panel 2, we have:

25 From New York Law School, Ari Ezra Waldman.

1 He's is a professor there, excellent;

2 Center for Democracy and Technology, we have
3 Joseph Jerome;

4 Institute for Public Representation, from
5 Georgetown University Law Center, we have
6 Lindsey Barrett;

7 And we have, from MSR Strategies, Mary Ross,
8 a co-author of the CCPA. Excellent.

9 All right, so rules again:

10 The panel has 20 minutes; so each of you have
11 5 minutes to -- basically, to open up and summarize
12 your testimony.

13 We have your testimony in front of us, we can
14 read it. So if you want to summarize, so we can ask
15 you questions, this will move a lot quicker.

16 All right?

17 So I'll let any/either one of you start.

18 Go ahead.

19 ARI EZRA WALDMAN: Great, thank you.

20 Thank you for inviting us here today, and
21 thank you for having this hearing.

22 My name is Ari Waldman. I'm a professor, as
23 people up here like to say, downstate.

24 But it's a pleasure and honor to be here.

25 The -- in my written testimony I go into

1 detail about what's wrong with the current system,
2 the need for substantive rules, the need to blend
3 procedure with substance.

4 And, the "information fiduciaries" concept,
5 I am one of those guys, as the panel -- one of the
6 members of the panel mentioned yesterday, who has
7 written about this, and formed the basis for the
8 "information fiduciaries" concept.

9 And I also talk in my written testimony about
10 one thing that I think is missing from the New York
11 Privacy Act, which is this concept of privacy by
12 design.

13 So, first, briefly, I'll talk a little bit
14 about those concepts, and then feel compelled to
15 respond to a couple of things that we heard about
16 last -- in our last panel.

17 The "information fiduciaries" idea is based
18 on this idea that we entrust our data with third
19 parties, these companies that are using our
20 information for profit.

21 There's been some talk that the
22 "information fiduciaries" concept is way too broad,
23 but, really, what it imposes are three simple
24 things: Duties of care, duties of confidentiality,
25 and duties of loyalty.

1 "Duties of care" are -- can be boiled down
2 to, are reasonable responsibilities, are re -- are
3 responsibilities to take reasonable steps to secure
4 individual data.

5 The "reasonableness" levels are taken
6 directly from tort law that we all learn from day
7 one in law school.

8 "Duties of confidentiality" are about keeping
9 our information -- keeping our information
10 purpose-oriented and minimized.

11 So I like to use the words from the GDPR:
12 Purpose limitation and data minimization.

13 "Purpose limitation" is this idea that you
14 only collect information for a specific purpose,
15 not -- and you can't use it for different purposes,
16 because users can't consent to multiple purposes.

17 And you only -- and "data minimization" is
18 the idea that you only collect so much information
19 as is necessary for that particular purpose.

20 And that's what "confidentiality" is about.

21 The biggest thing about the
22 "information fiduciaries" concept is duties of
23 loyalty, which essentially say, as you noted
24 earlier, that companies cannot act like con men.
25 They cannot bene -- use our data to our detriment.

1 Whether that's financial loss, embarrassment,
2 fear, anxiety, and so forth, all of these, also,
3 laid out by fiduciary concepts in tort law.

4 So these aren't so far afield from -- as
5 some -- as some might make us feel.

6 "Privacy by design," however, which is
7 outside the Privacy Act, and I think should be
8 inside, is this idea that companies should be
9 required to consider privacy issues from the ground
10 up, as opposed to tacking that on at the end.

11 And we can talk more in detail during the
12 question-and-answer session, or, in my written
13 testimony I discuss what that means more
14 specifically.

15 With respect to some of the ideas that we
16 heard in our previous panel, I think it's important
17 to set the record straight.

18 The members of the previous panel talked a
19 lot about the costs of regulation, but didn't cite
20 any evidence that the GDPR or the CCPA has actually
21 raised costs.

22 And to suggest that one is better for smaller
23 companies versus larger companies, I'm not sure
24 where we get this idea that all small companies are
25 doing great things.

1 Small companies can steal our data and harm
2 us as well.

3 The companies (sic) that created a flashlight
4 app, that also collected our GPS data, was a very
5 small company.

6 The previous panel also talked a lot about
7 supporting the SHIELD Act, which is, basically, a
8 security act, but security is only one small part of
9 privacy.

10 They talked a lot about customers wanting to
11 give over information for convenience, or for small
12 benefits, but they don't talk about the dark
13 patterns that websites use in order to illicit or
14 manipulate us into disclosing.

15 They talked a lot about wanting a federal law
16 as opposed to a state law.

17 Not only do states play a large role here,
18 but then the members of the panel opposed a proposed
19 federal law.

20 So it really means that, I'm not sure that
21 the people that they represent want any federal, or
22 any, type of privacy law.

23 And they talked about providing the services
24 for free.

25 But as we all know, nothing in this world is

1 free.

2 They're -- the -- instead of giving up our
3 dollars or our pennies, we give up our information,
4 and it's not free, to suggest that all of these
5 contexts, all of these platforms, are really for
6 free.

7 They talked about -- they talked about the
8 power that individuals, or the control that
9 individuals, have to just tell a first party -- a
10 first-party data collector that they don't want to
11 use -- they don't want their information used in
12 that -- in the ways that they have been.

13 But they don't talk about all the cognitive
14 biases that prevent us from saying no to those
15 companies.

16 And, finally, they talked very dismissively
17 about everyday New Yorkers trying to effectuate
18 their rights in court.

19 But, without seat -- without private rights
20 of action, we would not have gotten seatbelts, or
21 side-impact protection, in our cars.

22 So I think there are quite a few things that
23 we need to -- that we -- that are in this bill that
24 would actually protect New Yorkers.

25 LINDSEY BARRETT: Thank you.

1 Uhm, hi, I'm Lindsay. I am a staff attorney
2 and teaching fellow at the Institute for Public
3 Representation at Georgetown.

4 I have written on consumer privacy law and
5 Fourth Amendment, and a little bit on information
6 fiduciaries (indiscernible) with Ari's work and
7 other.

8 Today I hope to make four main points a
9 little more succinctly than I had originally
10 anticipated.

11 But, first, that privacy is ripe for
12 regulation by New York State. And this bill is an
13 important step for protecting people from digital
14 exploitation.

15 Second: Privacy rights are civil rights.

16 Lax laws, enabling abusive practices, have a
17 disproportionate impact on vulnerable groups. And
18 any effective privacy law must be based on that
19 understanding.

20 Third: Meaningful access, correction,
21 deletion, and transparency rights for individuals
22 are necessary for any comprehensive privacy law, but
23 insufficient without meaningful enforcement
24 capabilities to make industry take them seriously.

25 Finally: Characterizing data collectors as

1 information fiduciaries can go a long way towards
2 correcting the imbalance of power between companies
3 and the consumers they surveil.

4 I'm mentally surveying what to cut.

5 So as technology has made our lives easier
6 and more collaborative, it's also capable of making
7 them more vulnerable and more unfair.

8 People struggle to get even a vague sense of
9 what information companies collect about them and
10 how it's being used, through difficulty in
11 understanding the data ecosystem and making informed
12 privacy choices, is primarily due to two things:

13 The rapaciousness of an extractive ecosystem
14 of commercial surveillance unencumbered by any real
15 risk of punishment for bad conduct, and, the
16 uselessness of notice and choice as a method of
17 privacy governance, which provides neither notice
18 nor meaningful choice.

19 While the privacy laws we have rest on
20 consent, privacy settings and privacy policies do a
21 terrible job of obtaining informed and meaningful
22 consent.

23 The idea that people are empowered to protect
24 themselves online when a company announces its data
25 collection and use practices in convoluted

1 boilerplate has proven to be a fiction, both due to
2 the limitations of what privacy policies can really
3 accomplish and the cognitive limitations of human
4 beings.

5 Most people don't understand the invasive
6 potential of the technology they use, and the
7 privacy policies they encounter do a poor job of
8 explaining the risks.

9 Moreover, people encounter far too many
10 privacy policies to make reading them a feasible
11 decision.

12 The result is opaque disclaimers that no one
13 understands and no one reads, purporting to foster
14 informed privacy decision-making, when the result is
15 anything but.

16 Choice -- and Ari touched on this -- but
17 choice is also a misnomer when consumers barely have
18 any.

19 Companies also rely on selective disclosures
20 and manipulative product architectures to constrain
21 the little choice that consumers do have.

22 Many companies rely on dark patterns or
23 product design cues deliberately crafted to overcome
24 the user's conscious decision-making to the benefit
25 of the service operator and the detriment of the

1 user, coaxing them to share more money than they
2 intended, stay on the platform for longer, or spend
3 more money.

4 People are cajoled, badgered, and manipulated
5 into giving up their personal data.

6 It's no wonder that so many of them are
7 resigned to the prospect of it being misused.

8 Against this backdrop, we have tech companies
9 that have taken the lack of regulatory constraints
10 around the collection and uses of data and run with
11 it.

12 Our sectoral privacy laws are so cagily
13 defined, that many of the exploitive practices today
14 fail to fall under their ambit.

15 As congressional momentum to pass a
16 comprehensive privacy law slows, State action in
17 this arena is even more vital to ensure that people
18 are protected from digital exploitation.

19 Any effective privacy law must approach
20 privacy as a basic civil right.

21 The fact that the oceans of data collected
22 about each of us are used to fuel algorithmic
23 decision-making means that privacy isn't just an
24 issue of desiring solitude. It's a question of
25 basic fairness, and of limiting the bias and

1 discrimination that data collection can otherwise
2 fuel.

3 Weak privacy laws also disproportionately
4 disadvantage the poor.

5 Companies should not be able to offer
6 privacy-protected versions of a product for a fee,
7 and privacy-invasive product for free, anymore than
8 they should be allowed to offer lead-free paint for
9 a higher price than paint laced with poison.

10 It's coercive.

11 And basic consumer protection should not be
12 only available to the people who can afford them.

13 Privacy is not just a right to be let alone.

14 It's a civil right, and must be treated like
15 one.

16 And I'm deeply encouraged by the way the
17 New York Privacy Act responds to that reality with
18 its broad definition of "privacy risks" and its
19 constraints on profiling.

20 And, of course, you have my testimony, and
21 I can give examples, especially your questions about
22 the child protection.

23 That was our complaint, and very happy you
24 mentioned it.

25 Defining data collectors as fiduciaries is a

1 helpful step towards correcting the anti-consumer
2 skew of the privacy ecosystem.

3 One of the biggest problems of a sectoral
4 system of regulation, and the narrow definitional
5 scope of most U.S. privacy laws, is that the default
6 presumption is that a company owes nothing to its
7 users beyond adhering to narrowly-defined duties and
8 prohibitions.

9 In a regulatory system where the vast
10 majority of data practices aren't covered, the
11 standard operating procedure is, collect first, ask
12 questions later, which encourages invasive
13 collection practices and unfair uses of data.

14 Establishing duties of loyalty and care, as
15 this bill does, shifts that presumption.

16 The responsibilities are carefully delineated
17 in the bill, but by creating broader duties,
18 exploitative uses of the data that aren't
19 specifically defined in the bill may still be
20 covered by it, rather than almost certainly being
21 exempted.

22 Most of us are largely resigned to the power
23 that well-resourced companies have over us and to
24 the expansive window that they have into our
25 lives --

1 SENATOR THOMAS: Lindsey --

2 LINDSEY BARRETT: -- but we shouldn't have to
3 be.

4 And I'm done.

5 [Laughter.]

6 SENATOR THOMAS: All right.

7 Let's go, Joseph.

8 JOSEPH JEROME: Am I on? Can everybody hear
9 me?

10 SENATOR THOMAS: Yeah.

11 JOSEPH JEROME: Chairpersons Thomas and
12 Savino, thank you very much for giving me the
13 opportunity to testify today.

14 My name is Joseph Jerome.

15 I speak on behalf of the Center for Democracy
16 and Technology, a 25-year-old non-profit,
17 non-partisan, technology advocacy organization based
18 in Washington, D.C.

19 The goal of my testimony today is to echo
20 what my fellow panelists are saying, but also to
21 explain to you why privacy is important, and the
22 urgent need for New York to limit companies'
23 abilities to use and abuse our data.

24 Unregulated data processing has real-world
25 impacts that extend far beyond headlines about

1 Facebook, or, really, just generalized concerns
2 about online ad tracking.

3 There are a few areas where New York can
4 really help to curtail unfair and discriminatory
5 corporate behaviors.

6 First: "Take it or leave it" privacy
7 policies disadvantage low-income Americans.

8 The irony of "notice and choice" is that it
9 really, as Lindsey mentioned, gives people very
10 little choice about how they share personal
11 information.

12 Not using an app or service is not a real
13 option.

14 And this option is especially stark for
15 low-income Americans who rely on mobile
16 technologies, and often don't have the time or the
17 money to shop for better privacy protections.

18 Low-income customers are least able to pass
19 up incentive programs, like grocery store loyalty
20 cards.

21 These programs feed into data brokers, that
22 then profile and score people based on incomplete
23 information. And this affects people's
24 opportunities in ways that no one can understand.

25 You asked a question about advertising.

1 People can't really explain what's going on.

2 Second: Commercial surveillance technologies
3 take advantage of power imbalances.

4 Residents in New York City -- in a New York
5 City apartment building found themselves needing a
6 smartphone app just to get into the building's
7 lobby, elevator, or mailroom.

8 Five tenants had to go to court, just to
9 enter their apartments using good old-fashioned
10 keys.

11 New privacy laws compensate for these power
12 imbalances by creating costs to cavalier data
13 practices.

14 Third: I think location data sharing, in
15 particular, is exploitive, and it raises legitimate
16 safety considerations.

17 I want to stop and emphasize location data
18 for a moment here.

19 The reality is, that companies have been
20 utterly careless in how they collect, share, and
21 even sell our location information.

22 This information ends up in the hands of
23 stalkers, aggressive debt collectors, and, yes, the
24 watchful eyes of law enforcement, and it's used to
25 harass people.

1 Their recourse is limited.

2 The National Network to End Domestic Violence
3 advises abuse survivors who are concerned about
4 phone tracking, to simply turn their phones off.

5 No one should have to make the choice between
6 using a cell phone and being safe from stalking.

7 The reality here, is that the burden of
8 privacy cannot fall on consumers.

9 We need clear rules for what companies can
10 and cannot do with data.

11 My organization, CDT, we support a federal
12 solution to these problems.

13 But the reality is, as Congress delays and
14 delays, states must step into the breach.

15 And New York would not be an outlier here.

16 The California Consumer Privacy Act is also
17 not an outlier.

18 It joined state laws in Illinois, Vermont,
19 and Massachusetts that provide meaningful privacy
20 protections.

21 New York now has the opportunity to seize
22 this moment, to shape the national conversation
23 about what companies can do with our data.

24 What should a meaningful privacy regulation
25 have?

1 Let me offer five suggestions.

2 First: It must offer the ability for
3 individuals to access, correct, delete, and port
4 personal information.

5 Second: It should require reasonable data
6 security measures, and make companies responsible
7 for how they handle information.

8 Third, and this is where things get harder:
9 It should include explicit use limitations,
10 particularly around the repurposing and secondary
11 use of sensitive data.

12 Geolocation is a good example of this.

13 Fourth: It should deal with data-driven
14 discrimination and civil rights abuses.

15 And, finally: It has to provide for strong
16 enforcement.

17 If you do not have strong enforcement, the
18 most carefully drafted privacy law on the books will
19 not accomplish anything.

20 It is important that these components are not
21 watered down by definitions or provisions that
22 undermine the rule.

23 Lack of clarity invites corporate malfeasance
24 and exploitation, and overbroad exceptions create
25 loopholes that swallow well-intended privacy

1 protections.

2 That explains why you are hearing so much
3 about the need to both narrow the scope of personal
4 data, and also explain why you hear people say that
5 they want the broaden the definition of
6 de-identified data that can be excluded from
7 protection under the law.

8 Importantly, the New York Privacy Act
9 includes rigorous and meaningful definitions around
10 both of these things.

11 However, despite the fundamental problem, is
12 that companies should just not be put in the
13 position of deciding what privacy risks they need to
14 subject consumers to.

15 Despite the fact that this bill's language
16 around privacy risks draws from an industry proposal
17 from Intel, you still saw a tremendous amount of
18 pushback on the last panel.

19 The reality is, that rather than giving
20 businesses the discretion to determine whether their
21 data practices are risky or not, we need explicit
22 limits on what companies can and cannot do with
23 information.

24 My organization, CDT, has proposed privacy
25 legislation that limits certain data-processing

1 activities.

2 Location data is a good example of this, and
3 a good example of why restrictions are necessarily.

4 The New York Privacy Act and the SHIELD Act
5 both are great and strong first steps that address
6 the five components I mentioned.

7 OFF-CAMERA SPEAKER: It's time.

8 JOSEPH JEROME: And I look forward to taking
9 any of your questions.

10 SENATOR THOMAS: Mary.

11 MARY STONE ROSS: (Microphone turned off.)

12 Hi, it's an honor and a pleasure to be here,
13 and I commend you on the New York Privacy Act.

14 It's also a particular pleasure for me, as
15 I was born and raised in Albany, and I'm a proud
16 graduate of Shaker Heights.

17 My name is Mary Stone Ross.

18 I was one of the original proponents and
19 co-authors of the initiative that became the
20 California Consumer Privacy Act.

21 I'm no longer a part of that group, though,
22 so these are my own comments.

23 OFF-CAMERA SPEAKER: Can you use the
24 microphone?

25 MARY STONE ROSS: (Microphone turned on.)

1 Our country is becoming increasingly
2 polarized by the very technologies that were
3 supposed to connect us.

4 As a former CIA counterintelligence officer,
5 and counsel on the House Intelligence Committee,
6 I have a fundamental understanding of the power of
7 big data.

8 I've seen it firsthand used to disrupt
9 terrorist networks and stop human traffickers, but
10 I've also seen that power abused by governments, and
11 certainly by corporate interests.

12 Regulation must shine a light on what data is
13 collected, and grant consumers control over its use,
14 and remedies for its misuse, so our personal
15 information cannot be used to manipulate and divide
16 us.

17 It is possible to draft legislation that
18 protects consumers' privacy while balancing a
19 business's need to collect and use personal
20 information.

21 We accomplished this in California.

22 The CCPA gives all Californians:

23 First: The right to find out what's
24 collected about them and about their devices;

25 Second: The right to opt out of the sale;

1 And, third: Increases fines and penalties
2 for data breaches.

3 Transparency is the cornerstone of the entire
4 law, and should be the cornerstone of any good
5 consumer-privacy legislation.

6 Today, consumers are consenting to the
7 collection, use, and sale of their personal
8 information without truly knowing what they are
9 consenting to; not because they are ignorant, but
10 it's because it is effectively impossible to be
11 informed.

12 As "Atlantic" Reporter Alexis Madrigal found,
13 reading privacy policies you encounter in a year
14 would take 76 workdays.

15 Businesses have considerable expertise and
16 knowledge about the values and uses of our data;
17 therefore, in order for the consumer to grant
18 meaningful consent, the business should have the
19 burden to provide clear disclosures.

20 Oracle, a data broker, publishes a data
21 directory of over 40 sources of information that
22 they repackage and sell, including from all three
23 credit reporting agencies;

24 And, Solve, who verifies that someone is a
25 human from their caption network, which is the

1 "I'm not a robot."

2 SENATOR THOMAS: Right.

3 MARY STONE ROSS: Oracle also sells
4 information from Evite, the popular online
5 invitation service.

6 In the 2017 version of the data directory,
7 Evite says it uses its network of users, which
8 includes consumers who send, but also consumers who
9 receive invitations, including, if someone is
10 expecting a baby, if they are moving, traveling, or
11 if they are alcohol enthusiasts.

12 They are getting around the effective
13 Children's Online Privacy Protection Act (COPPA) by
14 collecting information about the age and presence of
15 children in the household from the parents, not from
16 the children.

17 Over a year ago, during the campaign, I was
18 interviewed by "Deseret News," and used this
19 example.

20 The reporter linked to the Oracle directory.

21 Evite refused to talk to the reporter, but
22 promptly had Oracle remove their entry.

23 Evite -- although I have a copy. You have a
24 copy too. (Indiscernible.)

25 Evite is hiding their actual business model

1 from consumers, because they can, and that they know
2 many consumers would be outraged if they found out
3 what actually happens.

4 Enforcement is key, and I'm glad the New York
5 law has robust enforcement.

6 Quite frankly, this was a mistake that was
7 made in the legislative compromise in California, as
8 the CA's Attorney General Office, who is now the
9 primary enforcer, predicts, that even with
10 additional resources, they'll only be able to bring
11 three enforcement actions per year under the CCPA.

12 It is possible to draft effective privacy
13 legislation that does not disrupt legitimate
14 business interests.

15 We drafted the CCPA with the understanding
16 that Silicon Valley and technology businesses in
17 California are important to our state's economy and
18 way of life; but, also, that some uses of data are,
19 in fact, good for consumers.

20 Thus, under the CCPA, we did not place
21 restrictions on the first-party's collection and use
22 of personal information.

23 We consciously crafted the CCPA to protect
24 legitimate business purposes, including fraud
25 detection, fulfilling orders, and even contextual

1 advertising.

2 Privacy, in fact, is good for business and
3 good for competition.

4 As Johnny Ryan, chief policy and industry
5 relation officer at Brave Software, a private and
6 secure browser, noted in his recent congressional
7 testimony:

8 "Today, Big Tech companies create cascading
9 monopolies by leveraging users' data from one line
10 business to dominate other lines of business too.

11 "This hurts nascent competitors, stifles
12 innovation, and reduces consumer choice.

13 "There are several successful businesses that
14 offer privacy-focused alternatives, and regulation
15 will encourage more."

16 I want to conclude with a note of caution.

17 Although the legislative deal in California
18 was struck in good faith, and all parties agreed
19 that some language needed to be cleaned up, there
20 are over 20 bills making their way in Sacramento
21 right now to weaken the CCPA.

22 Thank you for your time, and I look forward
23 to answering your questions.

24 SENATOR THOMAS: (Microphone turned off.)

25 I'll ask the questions.

1 So, thank you all for being here, and thank
2 you for the testimony that you just gave.

3 (Microphone turned on.)

4 I know all of you were in the room when
5 Panel 1 was testifying?

6 Did all of you hear what they were talking
7 about?

8 Okay.

9 So, first question here, right, it's the
10 first question that I asked them as well: How would
11 you define "personal data"?

12 MARY STONE ROSS: I can start.

13 I think that when you define "personal
14 information," it has to be much broader than what
15 they were talking about this morning.

16 I mean, look, like, this is me. (Holding up
17 cell phone.) This follows me absolutely everywhere.

18 As we see, as more and more people have
19 Internet things/devices --

20 We just bought a new dishwasher, and one of
21 the options was Wi-Fi-connected.

22 I don't know why you need a Wi-Fi-connected
23 device, unless it's going to load and unload itself
24 for me.

25 -- but, there are all of these devices that

1 are collecting information, and then transmitting it
2 back.

3 So it's very, very important that, it's not
4 just my name, it's not just my Social Security
5 number, but it encompasses all of these things.

6 JOSEPH JEROME: In our draft legislation, we
7 would propose a definition largely modeled after the
8 Federal Trade Commission, which includes any
9 information linked, or reasonably linkable, by a
10 business to a specific covered person, or, again,
11 consumer device.

12 Again, in the first panel, there was
13 reticence about broad definitions of "personal
14 information."

15 That's by design.

16 You absolutely need to have a law that
17 broadly covers a lot of information.

18 If we're talking about the New York Privacy
19 Act specifically I would imagine some of the
20 pushback has been around the words "related to."

21 Conceptually, the idea, in a personal
22 definition of "information related to" could
23 encompass everything.

24 That said, we would just caution about
25 need -- efforts to narrow it pretty extensively,

1 because, if you start having a definition that's
2 just name, plus some other stuff, it's not really
3 getting at the data-driven problems that I think all
4 of us have identified.

5 LINDSEY BARRETT: I would definitely echo
6 Joe's definition.

7 I also think the bill did a great job of kind
8 of encapsulating what Mary was mentioning, that, you
9 know, there are so many definitions of
10 information -- or, rather different kinds of
11 information that can be so revealing about each of
12 us.

13 One thing that I would consider in crafting a
14 definition, is not to just unilaterally exempt
15 publicly-available information from covered
16 information, by virtue of the fact that a lot of the
17 information that, you know, data brokers and others
18 get is from public records, and can be pretty rich
19 in depth, and, uhm -- yeah.

20 ARI EZRA WALDMAN: Just, very briefly, I --
21 I support the CDT's definition.

22 I would add that, vanguard legislation in
23 this space should account for the fact that
24 algorithms, based on large datasets, can take
25 seemingly innocuous, or non-personal, information,

1 and develop personal information.

2 Which is one of the reasons why legislation
3 has moved from simple PII (or, personally
4 identifiable information) which used to be just
5 names, e-mail addresses, you know, Social Security
6 numbers, and financial information, to a far more
7 broader definition.

8 And I think the New York Privacy Act gets in
9 that, moves in that direction.

10 We should make it explicit, that using
11 technological tools to develop personal information
12 or intimate information, especially information that
13 keys to protected classes, is also considered -- is
14 also going to be considered personal information,
15 even if the source of it, or the germ of it, were
16 seemingly innocuous pieces of data.

17 SENATOR THOMAS: Ari, you actually got into
18 this in your testimony.

19 You heard from the industry, they were
20 complaining that complying with these rules will
21 make it impossible for them do business.

22 Is this a fair concern?

23 ARI EZRA WALDMAN: So we hear the -- we hear
24 this concern a lot, that regulation will stifle
25 innovation, or will prevent companies from doing

1 their work.

2 It's a Republican talking point every time a
3 law is proposed in pretty much any legislative
4 chamber.

5 There is very little evidence that regulation
6 does stifle innovation.

7 There are several papers, both in the
8 economic and the political science and in legal
9 literatures, that prove that there is no evidence of
10 stifling -- stifling innovation.

11 Another piece that -- that -- another
12 piece -- another piece that that argument relies on,
13 is that it's harder for smaller companies to meet
14 compliance costs than it is for larger companies.

15 I think that misses the point that, as I was
16 arguing earlier, it's not necessarily better that a
17 company is smaller.

18 Two guys in a garage can invade our privacy
19 just as insidiously as a 40,000-person company.

20 The focus should be on, not the size of the
21 company, but in the purpose of regulation.

22 Regulation has the capacity to actually
23 inspire innovation, inspire the right kind of
24 innovation, or socially-conscious, or innovation in
25 line with what consumers want.

1 If -- someone -- someone came to me when
2 I was speaking in Brussels sometime ago, saying
3 that, Well, if we pass a law like this, we're never
4 going have another Facebook.

5 And my response was, "That's great."

6 [Laughter.]

7 ARI EZRA WALDMAN: I don't want another
8 Facebook that's damaging our democracy, or
9 endangering the lives of LGBTQ persons by pushing
10 them out of the closet, or endangering the lives of
11 women by allowing harassment to occur.

12 If we can pass a law that enhances the right
13 type of innovation, then that's great.

14 LINDSEY BARRETT: Yeah, I'm going to stop
15 just, you know, nodding along like a bobblehead to
16 everything Ari says, but, I would absolutely agree
17 with all of it.

18 And, in addition, it's funny that the talking
19 points that, my God, any law will completely kill
20 innovation in its cradle, you know, that's coming
21 from industry, and I think they're doing themselves
22 a disservice.

23 Like, if we're going to talk about, like, the
24 creative genius of American innovation, and all of
25 that, you know, give them a little credit.

1 I think that, you know, given -- given laws
2 defined like this one is, setting clear boundaries
3 and saying: No, this is bad, don't do that. This
4 is okay, go forth.

5 You know, of course, you can imagine that
6 they would harness that creativity, and respond.

7 And, you know, regulation would curb out the
8 exploitive practices and allow the good ones.

9 JOSEPH JEROME: I would just add that we hear
10 a lot about how the GDPR is impossible to comply
11 with.

12 I might push back and ask, whether these are
13 costs that companies should have been bearing to
14 begin with.

15 The GDPR, we should understand, replaced
16 existing data-protection laws that have been in
17 Europe for 20 years.

18 Not a whole lot changed.

19 What did change was, suddenly, there were big
20 fines and more enforcement which opened companies'
21 eyes.

22 So, we ought to, again, be asking ourselves,
23 whether some of these things, like privacy by
24 design, risk assessments, that the GDPR talks about
25 as accountability, were things that companies should

1 have already been doing.

2 Now, to the extent we think that that's too
3 wishy-washy and does have unfair costs, the
4 alternative is what CDT is approaching, is that we
5 just need to make clear restrictions on stuff you
6 can and cannot do.

7 And so, you know, again, I'll give you an
8 example.

9 We keep talking about the brightest
10 flashlight app.

11 Engine Advocacy, which is a non-profit
12 network of startups, told Congress that, you know, a
13 flashlight app has no clear functional need to
14 access a user's precise geolocation app to deliver
15 its service.

16 That's pretty obvious to, I think, everybody
17 on this panel.

18 We don't need to have risk assessments or
19 costly privacy attorneys to make that determination.

20 We should just say, in law, that apps don't
21 need to collect location data they don't need.

22 MARY STONE ROSS: And I would just add, from
23 personal experience, the opposition campaign that
24 formed to oppose the initiative was called the
25 Committee to Protect California Jobs and Promote

1 Innovation.

2 And -- which was, actually, Google, Amazon,
3 AT&T, and Comcast, and Verizon, until
4 Cambridge Analytica happened. And then Facebook,
5 and Verizon actually, also dropped out.

6 But -- so this is a scary tactic.

7 It's -- as I said in my testimony, privacy is
8 actually good for competition and good for business.

9 LINDSEY BARRETT: And, actually, you can talk
10 to the company, somebody -- one of you mentioned,
11 uhm, the Brave --

12 JOSEPH JEROME: Brave.

13 LINDSEY BARRETT: -- the Brave guy.

14 But, you know, Brave, DuckDuckGo, you know,
15 there are other companies that are rising up in --
16 you know, and making these business models that do
17 not rely on just surveilling people for no reason,
18 and keeping information that will likely have bad
19 effect for people.

20 So it's not impossible.

21 SENATOR THOMAS: Lindsay, in your opening
22 testimony, you wanted to talk about the privacy of
23 children, so let's get into that.

24 Should children have a greater privacy when
25 it comes to these applications that we use on our

1 phones and the websites that they use?

2 LINDSEY BARRETT: So I think there are two
3 things about kids -- well, there are a lot of
4 things.

5 But, first, you know, kids will do better in
6 an environment where there are strong protections
7 for everyone.

8 You know, kids will do better in an
9 environment where business is not incentivized to
10 assume that regulators will never come knocking on
11 their doors, and that our laws are so cagily defined
12 and rarely enforced, that nothing bad will ever
13 happen to them if they push the boundaries.

14 So, either way, in a better-regulated
15 ecosystem, kids will do better.

16 That said, by virtue of the fact that, you
17 know, we can talk about the cognitive limitations of
18 adults that hinder privacy decision-making, and
19 that's absolutely correct.

20 It's even more so for kids.

21 You know, kids don't know what they're
22 encountering.

23 There's all kinds of interesting research.

24 You know, kids see YouTube, and it's a brand
25 that they understand, so they say, Oh, no, I don't

1 think YouTube would collect anything.

2 You know, they trust it.

3 So there is a need to provide firmer
4 protections for children.

5 And there's also, when you're balancing kind
6 of, you know, different equities of, you know, where
7 should we draw the line for privacy protections, for
8 children, it seems like a pretty easy consensus to
9 reach, that, you know, kids are more vulnerable.
10 They're -- the need to protect them, and, you know,
11 for instance, for a right to delete, makes more
12 sense.

13 You know, they're -- they're -- and that's
14 not to undercut the case for why it makes sense for
15 adults.

16 But for kids who don't realize what they're
17 putting online, it's particularly important.

18 And the funny -- the other thing about kids,
19 and COPPA, is, on the books, COPPA is a pretty
20 decent law.

21 Like, it sets out some pretty firm
22 limitations, and gives parents access and deletion
23 rights.

24 But the fact is, because it's so
25 under-enforced, companies don't bother to collect

1 it.

2 So you mentioned our Amazon Echo Dot
3 complaint.

4 Amazon is a giant, behemoth tech company.
5 They have an army of compliance lawyers.

6 They have no reason not to comply with COPPA,
7 other than the fact that, you know what? The risks
8 of people bothering them -- rather, not us -- but,
9 the FTC bothering them about it, are pretty low.

10 So, COPPA's a great example of why it's so
11 important for privacy laws to have real enforcement,
12 and even things like a privacy right of action.

13 And why it's so great that the New York
14 Privacy Act does.

15 SENATOR THOMAS: Anyone else?

16 MARY STONE ROSS: One of the approaches we
17 thought about taking was expanding COPPA. But then
18 we decided that privacy is something that's
19 fundamental to every single consumer.

20 And COPPA is a good law.

21 I think, as I mentioned in my testimony, the
22 problem is, companies are getting around it by
23 collecting information about children from their
24 parents.

25 So any privacy laws should address that, and

1 make sure that doesn't happen.

2 And, absolutely, can't talk strongly enough
3 about the need for true enforcement.

4 LINDSEY BARRETT: And I also should have
5 mentioned, you asked about rights for minors
6 under 18.

7 You know, COPPA starts at 13.

8 It's not as though, all of a sudden, your
9 mental faculties are set in stone perfect at 12.

10 You know, adults still struggle to manage
11 their privacy rights, because it's impossible to do
12 for -- you know, on an individual basis.

13 So, yeah, in considering how to protect kids,
14 we still have, you know, 13 to 18, tweens, teens,
15 going out into the world and, unfortunately,
16 compromising themselves, because the law doesn't
17 protect them.

18 SENATOR THOMAS: I asked this question to the
19 last panel as well.

20 How long should a company hold personal
21 information?

22 ARI EZRA WALDMAN: A company should only hold
23 information as long as they need it for the
24 particular purpose for which they collect it.

25 This is the principle of data minimization

1 and purpose limitation.

2 And I'd add in privacy by design.

3 So, for example, we should have -- we need a
4 rule, and the Data Protection Working Board in
5 Europe, which is a group of leaders that has -- that
6 contributed to writing the GDPR, and now issue
7 reports interpreting it, have said that: When you
8 put together purpose limitation and data
9 minimization and privacy by design, what we have is,
10 not just collection for particular purposes, but,
11 also, in databases that are automatically -- that
12 are built so they automatically delete data after a
13 year, after two years, instead of promising that,
14 we'll delete your data after a certain amount of
15 time.

16 So, all of those rules working together;
17 these duties of confidentiality and duties of design
18 work together, to protect individual data far better
19 than just putting something in a privacy policy that
20 says, we promise to delete your data after a certain
21 amount of time.

22 MARY STONE ROSS: And I would also just add,
23 companies should be encouraged to only collect the
24 information that they actually need to collect to
25 perform whatever function or service that they say

1 they're going to do.

2 So, I mean, going back to the flashlight
3 example, because it is so egregious, right, like,
4 only collect -- I mean, I don't even know what a
5 flashlight app needs to collect, other than to know
6 that, turn on that button there. But they certainly
7 don't need to collect your location information.

8 JOSEPH JEROME: So I will tentatively agree
9 with the previous panel, that it's difficult to say,
10 and it might depend on context.

11 The challenge is, as advocates, we often
12 don't know how long these companies are retaining
13 it.

14 They use general terms of, you know,
15 "legitimate business interests," "reasonable
16 retention periods."

17 It would be useful to have more of an
18 understanding from industry groups, across sectors,
19 about how long they actually need some of this
20 information for.

21 We spent a lot of time, again, talking about
22 online advertising.

23 It's my general understanding that a lot of
24 ad data is capped for 13 months, because that gives
25 you a year, plus a month, to sort of measure

1 advertising campaigns over a year.

2 But that's sort of my internal knowledge and
3 discussion of it. It's not something I think people
4 are broadly aware of.

5 And when we talk about things like location
6 data, again, we need to have a more -- a fuller
7 conversation.

8 And we're already starting to see some of
9 this.

10 I mean, Google has rolled out the ability to
11 auto-delete some of your location data after, you
12 know, 3 months, or 18 months.

13 Those seem like good numbers to me, but
14 they're sort of arbitrary.

15 Do you need location data for 3 months? Do
16 you need it for 18 months?

17 I don't know.

18 And companies need to be doing a much better
19 job of sort of justifying this.

20 LINDSEY BARRETT: And I'll actually
21 (indiscernible) point from the previous panel, which
22 is that you can't -- well, I'll add a point: You
23 can't abuse data that you haven't collected. But,
24 also, data that you haven't collected can't be
25 hacked.

1 SENATOR THOMAS: That's true.

2 Thanks.

3 Next, I'm going to combine the first panel
4 and second panel together, so we will have a more
5 lively discussion here.

6 Should companies be able to tell users that
7 they don't agree -- like, if they don't agree to
8 share, then they cannot receive the services?

9 ARI EZRA WALDMAN: No.

10 They're -- to deny individuals access to a
11 service, simply because they have actually exercised
12 their preferences with respect to data, is
13 discrimination.

14 We've noted this -- members of this panel
15 have noted how the burdens of sharing information
16 are disproportionately borne by members of
17 marginalized groups; whether it is the poor; or
18 whether it is individuals, maybe queer individuals,
19 who are reaching out for online community, where
20 they can't find community in their geographic area.

21 When data burdens are borne by marginalized
22 populations, that means that you're going to get
23 access to, and you allow companies to discriminate
24 on who's going to get better access to a platform,
25 that means you're going to bifurcate the Internet

1 between the haves and the have-nots.

2 I don't think anyone really wants that.

3 I think companies want the freedom to be able
4 to do that, because they want to encourage
5 individuals to see their data.

6 But that's just yet another design tactic
7 that companies use to disempower individuals.

8 And they're allowed to it under the current
9 system.

10 It's clear, and it's hard to argue against
11 this idea, that companies should be able to
12 discriminate against their users.

13 And when I hear companies suggest that they
14 should be able to manipulate users into giving over
15 information, it's just an attempt to disempower
16 users even more.

17 MARY STONE ROSS: I was going to say that
18 privacy should not be a commodity that only the
19 wealthy can afford.

20 And, especially, a lot of these privacy --
21 the worst abusers -- abuses are low-income, more
22 vulnerable, classes of people.

23 And then, also, just another note of caution,
24 this was something that really got messed up in the
25 legislative deal in California.

1 So in the initiative, we had a really strict
2 non-discrimination provision.

3 So it said that a business would not be able
4 to deny access, charging more, if you exercised any
5 of your rights under the California Consumer Privacy
6 Act.

7 So it was the right to opt out, but even just
8 all the transparency, the right-to-know piece of it.

9 So in the legislative compromise, the
10 non-discrimination language was still there, but
11 there was some, just -- industry was pushing back.

12 And there was some typographical errors about
13 who had to say the value of the data, and who the
14 value of the data was for.

15 So there was, you know, like agreement that
16 this needed to be cleaned up.

17 So, now, that bill has become a
18 "customer-loyalty program" bill that eliminates any
19 mention of non-discrimination. And, in fact, the
20 legislative intent talks about how much Californians
21 love their loyalty programs.

22 Personally, I hate going into Safeway
23 because, if I don't put my phone number in, it's
24 twice as expensive as going to Whole Foods.

25 And so these are things that, you know, like,

1 you need to go in, eyes open, that they're going to
2 push for these loyalty programs, but it's
3 discrimination.

4 JOSEPH JEROME: I would just add that, the
5 pay for -- the question about pay for privacy and
6 pay for privacy programs, it is very loaded, because
7 there's a lot of different business models and a lot
8 of different stuff going on.

9 I won't -- my panelists -- co-panelists have
10 done a good job of describing how it is incredibly
11 discriminatory.

12 You mentioned grocery store loyalty programs.

13 I think loyalty programs do provide a
14 tremendous amount of value to consumers when they're
15 first-party loyalty programs, when the store is
16 actually trying to do things to make me to come
17 back, and to develop a relationship with me.

18 The problem with so many of these loyalty
19 programs, as I mentioned in my written testimony, is
20 that they are simply a pipeline to sell data to data
21 brokers.

22 So if I want to access cheap milk at the
23 grocery store, I need to have a loyalty card. That
24 loyalty card is going to be run by a company I've
25 never heard of, who's then going to have a data

1 co-op, and share more and more information around.

2 And that's going to be used in ways that are,
3 either, discriminatory, or we just don't know,
4 because there's no requirement that they tell us.

5 And, that, I think is the real problem in our
6 data ecosystem.

7 MARY STONE ROSS: And, sorry, just to echo
8 that point about loyalty programs, the business is
9 getting a benefit from you being a part of that
10 loyalty program.

11 For example, on airlines, if you're a member
12 of their loyalty program, you know, like, that's the
13 pipeline that you're going to go to. And, most
14 likely, you're going to come back to them.

15 So selling your information on top of it is
16 just extra ice cream.

17 SENATOR THOMAS: I asked this with the last
18 panel as well.

19 Is there anything that I should do to improve
20 the New York Privacy Act?

21 LINDSEY BARRETT: I -- I -- so I would take
22 out the exception for publicly-available
23 information, by virtue of the fact that so much of
24 what data brokers rely on is from public records.

25 You know, you can get both -- you take

1 information that by itself seems innocuous, but, in
2 combination with (indiscernible), a grocery store,
3 now I know, you know, oh, you purchased a pregnancy
4 test here, but then didn't buy diapers a year after.

5 You know, whatever you can get from that, you
6 combine that with, I don't know, publicly-available
7 arrest records, driver's records; there's all kinds
8 of publicly-available information that, as a
9 concept, it seems like, oh, it's out in the world,
10 there is no privacy interest there.

11 But, in combination with other information,
12 can be used in a very privacy-invasive way.

13 In my testimony I cite to Woody Hartzog's
14 work on public information.

15 Really illuminating.

16 And the other that I would add is, in the
17 except -- there's an exception for the liability
18 of -- this is a little bit into the weeds -- but,
19 "for the violations of third parties, absent actual
20 knowledge that the party planned to break the law
21 when the data was actually shared."

22 And I think that that will end up exempting
23 almost all transactions, because, usually, you know,
24 whatever, your Facebook, you make a contract with
25 GSR and Cambridge Analytica. You don't know at the

1 time that they are planning to go, and, you know,
2 break (indiscernible cross-talking) --

3 SENATOR THOMAS: What section is that?

4 LINDSEY BARRETT: This is a great question.
5 It might be in my testimony, and I can find
6 that and follow up.

7 SENATOR THOMAS: Okay. Thank you.

8 Anyone else?

9 JOSEPH JEROME: So I think Ari and Lindsay
10 are perhaps bigger fans of the "data fiduciary"
11 concept than my organization is.

12 You know, again, we would ask for explicit
13 limits around certain types of information, whether
14 it's health information or geolocation.

15 That creates a clearer rule for companies.

16 There's no confusion if you just can't do
17 certain things.

18 But I actually will say, that I think a lot
19 of what I would encourage you to sort of tow the
20 line on, is there are very good and strong
21 definitions in this law.

22 I mentioned briefly in my testimony how --
23 the definition of "personal information" and the
24 exceptions to that.

25 So, de-identified information is really the

1 ball game with these laws.

2 How those two definitions are scoped,
3 determines the scope of the protections.

4 And I think you have a really strong start
5 with those definitions, and I think you're going to
6 get a lot of pushback because of it.

7 ARI EZRA WALDMAN: I think this is a really
8 good start.

9 There are three things that I would focus on
10 in terms of potential changes.

11 One would be, with respect to the "fiduciary"
12 section, to make it a little bit more clear about
13 what the duties of information fiduciaries are.

14 And I laid those out in my written testimony,
15 as well as discussed it briefly here, duties of
16 care, duties of confidentiality, and duties of
17 loyalty; and describe briefly what that is.

18 And the Data Care Act does a nice job of
19 that, and there might be a good parallel.

20 I would also note, just as an aside, that
21 that is not inconsistent with the Delaware corporate
22 law's requirement that companies have fiduciary
23 duties to their shareholders.

24 There are -- just because a company has a
25 fiduciary duty to their shareholder doesn't mean

1 that they have other duties.

2 Products liability, for example, is a really
3 good example. Companies have duties to consumers
4 beyond just duties to their shareholders.

5 A second thing that I would suggest, that
6 we -- there might -- there's room for a discussion
7 on the role of privacy by design; the idea that
8 privacy should be part of the design process.

9 I've written quite a bit about this, as well
10 as some others, of what that actually means.

11 And I think there is a far better way to do
12 it than to just write Article 25, what the GDPR has.

13 And I talked about that in my written
14 testimony, of a more specific way that companies
15 can -- that provides notice to companies about what
16 "privacy by design" is.

17 And then, third, I agree with, about the
18 importance of these definitions.

19 But I also think that we could be even
20 stronger with private rights of action and
21 enforcement.

22 We shouldn't burden the New York Attorney
23 General's Office with the responsibilities for
24 protecting every element of privacy rights of
25 New York residents.

1 And there is such a strong capability for
2 private rights of action to have an effect on
3 corporate behavior, that there may be a role for,
4 and I think there is a strong role for, private
5 rights of action for individuals to effect their
6 privacy rights.

7 MARY STONE ROSS: I have a lot of notes,
8 which I'm happy to share with your office, because
9 they're pretty detailed.

10 But one thing that I would say, that you got
11 a lot of pushback from the first panel this morning,
12 but, it is critical to say that harm is a privacy
13 injury. That you do not tie it to a market-based
14 harm approach.

15 That approach is antiquated, and it doesn't
16 work in the privacy context.

17 And so you already have language in there,
18 which is fantastic, and I commend you for that.

19 The only thing that I would add is that, in
20 the California law, we allow a third party to
21 opt out on a person's behalf.

22 And the reason why this is important is, as
23 you can see with that Oracle data directory, there's
24 so many companies out there that are collecting,
25 processing, and selling your personal information,

1 and an individual has no idea who these companies
2 are.

3 So it would be great, speaking of another
4 business opportunity, or a non-profit opportunity,
5 to allow other people or organizations to be able to
6 opt out of the sale of your information on your
7 behalf.

8 SENATOR THOMAS: Thank you.

9 I'm going to hand this over to Senator Savino
10 now for some questions.

11 SENATOR SAVINO: (Microphone turned off.)

12 Thank you.

13 I'll be brief, because this is complicated,
14 very complicated, but illuminating.

15 (Microphone turned on.)

16 And it's almost as if people -- consumers
17 have become willing participants in the loss of
18 their own data, just by virtue of signing up for
19 rewards programs.

20 I mean, I know I'm guilty of it, we all are,
21 because people like to get things, as you --
22 I think, Mr. Jerome, you pointed out, that people
23 like their rewards programs.

24 We all do, because we get something tangible
25 of a benefit.

1 But it does kind of strike me as weird.

2 Like, I go into CVS and, you know, you swipe
3 your little card, and they give you this -- you ever
4 go to CVS and you get your receipt, it's like 4 feet
5 long, and it's all the coupons, because they know
6 your buying history.

7 Everything you've ever bought in the past
8 six months, and they're giving you a coupon for it.

9 And then the next thing you know, you go
10 home, and you log on, and, suddenly, there's a
11 coupon for that product.

12 And it is a little frightening.

13 But more frightening is, I'm looking at
14 this -- on the location service.

15 So my staff member behind me just gave me her
16 Google locator. And I'm looking at December 15th
17 of -- December 8th of 2015, her entire day.

18 Even though you can delete some of it, but
19 it's really hard to get rid of this.

20 Every moment of the day, where she was, what
21 she was doing.

22 How many minutes she spent driving in a car
23 from her address to Rite Aid.

24 And going to a college, and then going
25 somewhere else.

1 That's really scary.

2 What possible reason could they have to keep
3 all this information for all this time?

4 Why would they need to know where I was at
5 every moment of a day?

6 MARY STONE ROSS: I mean, the problem is,
7 right now, why wouldn't they keep all that
8 information?

9 It's free to hold on to it, and, who knows?

10 Like, maybe there's some use that they
11 haven't thought of yet to keep it.

12 So that's why we need regulation, to shift
13 that, so there is some cost to holding on, and
14 collecting all of that information in the first
15 place.

16 SENATOR SAVINO: I mean, I think, in some
17 respects, there's a value to -- to myself too.
18 Like, sometimes I forget what I was doing.

19 I go back to my calendar. You know, and as
20 an elected official, it's important, sometimes you
21 need to match up what you did on a particular day,
22 if you're filing your financial disclosure forms or
23 your filing campaign finance forms.

24 But it never occurred to me that Google
25 locator had my every moment in their system,

1 somewhere.

2 MARY STONE ROSS: And, also, that's your
3 calendar, so you should be able to go back and look
4 at it.

5 But do you want Google and 50 other tracking
6 services, and then, whoever else, to be able to look
7 at that information too.

8 SENATOR SAVINO: I think the point I'm trying
9 to make is, most people probably have no idea.
10 Right?

11 So you sign up for, you know, you get a
12 Google account.

13 You sign up for rewards at CVS or Rite Aid or
14 Macy's, or wherever it is that you do.

15 You do these things because you think that
16 there's a benefit to you personally, and you get
17 something out of it. You get coupons; you get
18 discounts; you get Macy's books; you get, you know,
19 the 4-foot-long receipt with, you know, extra bucks,
20 or whatever they call it at CVS.

21 So you get something of value.

22 But -- so consumers really have no idea that
23 they're doing this.

24 So -- so how do we -- beyond the passage of
25 this bill and enforcement --

1 Which I'm not sure how we would do that,
2 that's another challenge.

3 -- how do we raise awareness among consumers
4 that they need to be more vigilant with their data
5 protection on their own?

6 ARI EZRA WALDMAN: So it's not just that
7 consumers aren't aware.

8 And it's -- if consumers were just not aware,
9 then public-awareness campaigns would be effective.

10 But it's that these processes engage our
11 psycho -- innate psychological barriers to actually
12 understanding it.

13 Part of the problem is, one of the things we
14 call "hyperbolic discounting."

15 It's, humans are really, really bad at
16 comparing current benefits, like the loyalty or the
17 discounts that you get from a loyalty program, with
18 the -- with potential future risks.

19 We just can't adequately balance or assess
20 the risk and reward -- the risk-and-reward basis.

21 So, given that, then we can't really -- we
22 shouldn't really be focused on giving users more
23 information, or giving them more control, or giving
24 them more choice, because it's a fallacy.

25 That's what the current law does, and that's

1 what all transparency laws do, is just to say, give
2 users more information about what's happening.

3 That's why the structure of laws, like the
4 New York Privacy Act; or laws like, structures of
5 information fiduciaries; or any other -- or privacy
6 by design, are focused on shifting the burden of
7 protecting our privacy from individuals to
8 companies.

9 So, you ask, how do we help consumers protect
10 their privacy better?

11 Sure, we can educate, we can put it in
12 curriculum in schools. We can have campaigns about
13 it.

14 But that's not the goal.

15 We have to shift the burden to companies, and
16 provide regulation that limits what they can
17 collect, because we are cognitively unable, even
18 with all possible information, to make those
19 adequate choices.

20 SENATOR SAVINO: Hmm, interesting.

21 LINDSEY BARRETT: Yeah, I would echo that
22 1 million percent, and also say that, when we talk
23 about privacy, I think we tend, and I say this, in
24 that, it's become accidental by virtue of very
25 deliberate crafting of, kind of, talking points and

1 messaging from companies that don't want privacy
2 regulations.

3 But, we talk about privacy, in terms of
4 consumer protection, in a completely different way
5 than we talk about any other areas of our lives.

6 Like, we talk about, like, oh,
7 (indiscernible) -- you know, aren't we willing
8 participants, except, oh, by the way, you know, we
9 lack choice. This is in -- you know, it's an area
10 where people aren't able to deal with things.

11 But we don't say, like, oh, well, you know,
12 you seem perfectly willing to go out and buy spoiled
13 meat.

14 Like, we don't say, oh, that's what the
15 market will bear.

16 We say, no, there's a basic line of what
17 people shouldn't be able to subject themselves to.

18 So I think when we get bogged down too
19 heavily in kind of the willingness and the
20 expectations portion, where, part of it, there's
21 absolutely a grain of truth to it, but there's also
22 an extent to which it blurs the larger truth of the
23 extent to which these aren't, you know, harms that
24 people are able to avoid on their own.

25 And we talk about privacy in a weirdly, just,

1 categorically different way than we do other areas
2 of consumer protection.

3 JOSEPH JEROME: Yeah, I think I'm just
4 echoing what my co-panelists said.

5 I mean, the reality is, companies are happy
6 to provide us with longer notices and more choices
7 because we are drowning in notices and choices.

8 And, you know, as a privacy advocate, we have
9 Data Privacy Day once a year, and I'm always called
10 upon to -- by the media and other: What can I do to
11 protect my privacy?

12 And I'll say something, like, You know, check
13 out all of the apps and privacy settings on your
14 phone.

15 The average person has 80 apps on their
16 phone.

17 That's -- even at 5 minutes apiece, how are
18 you going to make the time for that, and we've just
19 handled the phone.

20 We haven't handled any the smart devices in
21 your home.

22 We haven't dealt with any of the
23 brick-and-mortar loyalty cards.

24 We haven't dealt with what employers are
25 doing with your data, what your health companies --

1 or, insurers are doing with your data.

2 You mentioned CVS coupons.

3 I'm always fascinated by what happens when
4 you use your CVS loyalty card at the CVS pharmacy.

5 We act like we have health privacy laws, but,
6 all of our privacy laws, in general, are very, very
7 leaky, and our health, you know, information falls
8 out of the HIPPA, which is the federal health
9 privacy law, pretty easily.

10 We spend a lot of time talking about how
11 financial data is very heavily regulated, but the
12 privacy protections around financial data are
13 minimal. You have to go to your bank and see if you
14 can figure out what choices you have about how they
15 share your financial data.

16 It's easier said than done.

17 And so I'm just, you know, parroting what
18 both Ari and Lindsey have said.

19 Individuals can't do the job.

20 Lawmakers need to start making some decisions
21 (indiscernible cross-talking).

22 SENATOR SAVINO: Well, truthfully, they mail
23 it, like, they send it to you. Right?

24 Most of us, we look at it, and then we just
25 toss it because it's, like, 14 pages and it's very

1 tiny type, and you're just like, ack, and you throw
2 it away.

3 Yeah, you're right. It's we -- you may be
4 right, we may not be able to cognitively absorb it
5 and internalize it.

6 MARY STONE ROSS: So one of the ways we
7 addressed this in California is that, if a business
8 is selling personal information, because there is an
9 opt-out, they have to have a button on the bottom of
10 their page that says, "Do not sell my personal
11 information."

12 So it's kind of a public shaming.

13 So AT&T, which you're paying for every month
14 for crappy service, who is also selling your
15 personal information, all of a sudden, when you go
16 to pay your bill, there would be a button on the
17 bottom of the screen that says, "Do not sell my
18 personal information."

19 And so what we've seen is that, businesses
20 who don't want to -- who don't want to be selling
21 your personal information are making sure that they
22 are compliant, so they don't have that button on the
23 bottom of the screen that actually calls them out on
24 what their business model is, in fact.

25 SENATOR SAVINO: And does the California law

1 have a private right of action?

2 MARY STONE ROSS: No, it got taken out.

3 It has a private right of action for data
4 breaches, but it got taken out in the legislative
5 compromise.

6 So this is the problem now.

7 It's just AG enforcement for most of the law.
8 And their office came out and said, they only think
9 they can only bring three enforcement actions under
10 the CCPA, a year.

11 But what the initiative had besides the
12 private right of action, is we also allowed district
13 attorneys and city attorneys and city prosecutors to
14 bring action under the law.

15 SENATOR SAVINO: Have any of them done that?

16 MARY STONE ROSS: It's not in effect yet.

17 January 1, 2020.

18 JOSEPH JEROME: Sorry to interrupt you.

19 I actually do think more enforcement
20 mechanisms is incredibly important.

21 And my organization was really involved in
22 the Washington Privacy Act, which had a lot of other
23 really strong ideas, but would have, basically,
24 preempted, again, local, county, and state
25 officials.

1 And, localities are really playing an
2 important role in the privacy debate.

3 The Los Angeles Attorney is bringing a
4 lawsuit against the Weather Channel app for, again,
5 selling location data.

6 We've seen the Washington, D.C., our attorney
7 general, is suing Facebook, pretty successfully so
8 far.

9 So, again, I think it's important to have
10 avenues of enforcement, and making sure that this
11 isn't just on the attorney -- the state attorney
12 general is vitally important.

13 LINDSEY BARRETT: And not to mention, Ari
14 mentioned this briefly, but, on the, kind of,
15 private right of action, every time you have an
16 industry panel, they'll say, Oh, my God, you know,
17 we'll be drowning in lawsuits.

18 But you also think about, kind of, the
19 incentives against people filing lawsuits.

20 They're expensive, they're difficult.

21 Most people don't do that.

22 The way that -- the reason that having a
23 private right of action is important is, one, if
24 there are problems of such a broad scale that it
25 does become, you know, reasonable and meaningful for

1 someone to pursue that, it's available.

2 But, also, it says to the companies, no, this
3 is real. You have you to take it seriously. This
4 isn't another privacy law that you can, you know,
5 laugh off because, oh, by the way, you know, the
6 state AG is already swamped, the FTC is swamped, you
7 know, they're not going to do anything about it.

8 So, in terms of gauging what's actually going
9 to happen, like, the way that having a private right
10 of action shapes incentives is vitally important.
11 And the odds of, you know, having every Tom, Dick,
12 and litigant waltz in and ruining American industry
13 is pretty slim.

14 SENATOR SAVINO: Uh-huh, that's true.

15 And we always hear that whenever we're
16 looking to improve people's ability to bring a
17 lawsuit.

18 Generally, trial attorneys don't take cases
19 unless there's merit to them, because they don't get
20 paid unless they win, so they have to put the effort
21 into it.

22 But, it's a valid point.

23 Yes?

24 MARY STONE ROSS: And just going back to why
25 we had a private right of -- I mean, there's a lot

1 of reasons why we had a private right of action in
2 the initiative form.

3 But one of the examples that was really
4 foundational to me, was there's a case going against
5 Facebook right now, that's progressing through the
6 courts, based on an Illinois Biometric Information
7 Privacy Act.

8 And so Texas actually has a very similar law,
9 but, in Texas, it's only AG enforcement, while, in
10 Illinois, it was AG enforcement, but also a private
11 right of action.

12 And so we see nothing -- both of these laws
13 have actually been on the books for many, many
14 years.

15 Texas, nothing happened.

16 But, in Illinois, they're making quite a bit
17 of progress.

18 SENATOR SAVINO: Hmm. Very good.

19 Thank you.

20 SENATOR THOMAS: All right, thank you all.

21 Panel 2 is dismissed.

22 (All panelists say "Thank you.")

23 SENATOR SAVINO: See, they knew I was talking
24 about them.

25 My Macy's money is about to expire, they just

1 sent me. They heard me.

2 [Laughter.]

3 SENATOR SAVINO: They heard me.

4 SENATOR THOMAS: All right.

5 So we have the third panel here.

6 Again, if I slaughter anyone's name, please
7 forgive me.

8 So, from Consumer Reports, we have
9 Charles Bell;

10 And from the New York Civil Liberties Union,
11 we have Allie Bohm.

12 So the rules, again, actually, since there
13 are only two of you, you're only going to be given
14 10 minutes, 5 minutes each.

15 So, let's start with Allie.

16 ALLIE BOHM: Thank you for the opportunity to
17 testify today.

18 My name is Allie Bohm. I'm a policy counsel
19 at the New York Civil Liberties Union.

20 Oh, that thing moves.

21 It is no longer possible to participate in
22 society without providing personal information to
23 third parties that may, in and of itself, reveal
24 intimate details of one's life, or, that when
25 combined with other data and analyzed, may expose

1 such information.

2 The consequences can be profound.

3 For example, personal information has been
4 leveraged to ensure that only younger men see
5 certain job postings, and to exclude
6 African-Americans from viewing certain housing
7 advertisements.

8 Cambridge Analytica obtained more than
9 50 million Facebook users' personal information, and
10 purported to use that information to convince
11 individuals to vote for Mr. Trump.

12 During the 2016 election, personal
13 information was also used to target ads to
14 African-Americans, urging them not to vote.

15 Against this backdrop, the Committee's
16 consideration of online privacy and the state
17 Legislature's role in overseeing it could not be
18 timelier.

19 Because of the limited time, I will describe
20 the scope of the problem and the legal landscape
21 that any privacy legislation will fall into.

22 My written statement talks about lessons
23 learned from other -- from our sister states, as
24 well as provides specific feedback on
25 Senator Thomas's New York Privacy Act.

1 We started our privacy work at the NYCLU by
2 making a list of harms that stem from the pervasive
3 collection, retention, sharing, monetization, use,
4 and misuse of personal information.

5 Here are some of them.

6 Entities, whether businesses, employers,
7 schools, landlords, health insurers, or
8 credit-issuing agencies, can use amassed personal
9 information to limit individuals' awareness of and
10 access to opportunities.

11 Depending on the opportunity, personal
12 information and sophisticated algorithms can be used
13 to circumvent our civil and human rights laws, as
14 I described earlier.

15 Even when advertisers do not deliberately
16 discriminate, individuals' opportunities may be
17 inadvertently limited as the result of the online
18 advertising industry functioning as intended.

19 For example, a representative of the Network
20 Advertising Initiative testified at November's
21 Federal Trade Commission hearing that, quote, Women
22 are less likely to see employment ads for careers in
23 the science, technology, engineering, and math field
24 simply because they have higher value to other
25 advertisers because women do more shopping.

1 In addition, as entities increasingly turn to
2 sophisticated algorithms to place ads, screen
3 resumes, or even in government hands to make bail or
4 child-custody decisions, the training data used to
5 develop the algorithms have outsized impacts on
6 individuals' opportunities and outcomes.

7 Algorithms work by identifying correlation,
8 not causation, and the training data used to, quote,
9 teach algorithms what patterns to look for, often
10 reflect and magnify entrenched historical biases.

11 In addition to discrimination based on
12 protected classes, amassed personal information can
13 be used to engage in unfair price discrimination.

14 Pervasive collection and use of personal
15 information can also exacerbate information
16 disparities and contribute to the erosion of free --
17 of trust -- (makes verbal sound) -- the erosion of
18 trust and free expression.

19 I'm trying to go too fast.

20 Collection and pooling of personal
21 information creates treasure troves for government
22 access. This is because the antiquated third-party
23 doctrine permits the government to get information
24 from third-party custodians without court oversight
25 and without ever telling the individual to whom the

1 information pertains.

2 It also creates a bull's eye for data
3 thieves, whether those seeking profit or those
4 seeking to interfere in U.S. elections.

5 Data breaches, and the misuse of personal
6 information, can lead to financial harm,
7 reputational harm, emotional harm, or physical harm.

8 It can undermine an individual's job
9 prospects, or family and friend relationships, and
10 can increase the risk of future harms.

11 Compounding these problems, individuals do
12 not know or consent to the manner in which entities
13 collect, use, retain, share, and monetize their
14 personal information.

15 Moreover, entities that collect, use, share,
16 retain, and monetize personal information have
17 specialized knowledge about the algorithms and
18 data-security measures they use, as well as about
19 how they collect, use, retain, share, and monetize
20 personal information, that the average individual is
21 unlikely to know or understand.

22 Still, individuals demonstrate time and again
23 that they care about privacy.

24 92 percent of Facebook users alter the social
25 network's default privacy settings, indicating that

1 they wish to choose with whom they share personal
2 information.

3 Similarly, 92 percent of Americans believe
4 companies should obtain individuals' permission
5 before sharing or selling their personal
6 information.

7 Drafters seeking to author privacy
8 legislation are not painting on a clean canvas, and
9 any legislation must be crafted to interact well
10 with existing New York and federal sectoral privacy
11 laws.

12 Moreover, comprehensive privacy legislation
13 must be tailored carefully to comport with
14 Supreme Court precedent.

15 In *Sorrell v. IMS Health, Inc.*, the Court
16 held, that speaker-based restrictions on the sale,
17 disclosure, and use of personal information to
18 heighten scrutiny, any privacy law that prescribes
19 the collection, use, retention, sharing, or
20 monetization of personal information, based on the
21 purpose for the leveraging or the identity of the
22 entity doing the leveraging, is likely suspect.

23 The NYCLU appreciates the opportunity to
24 testify today, and apologizes for speeding through
25 this, and stands ready to assist -- to answer any

1 questions, and also to assist the Committee,
2 Senator Thomas, and other interested lawmakers, as
3 you craft privacy legislation for New York State.

4 SENATOR THOMAS: Charles.

5 CHARLES BELL: Chairman Savino,
6 Chairman Thomas, thanks so much for the opportunity
7 to speak today.

8 My name is Chuck Bell. I'm programs director
9 for Consumer Reports, an independent, non-profit,
10 member organization representing 6 million consumers
11 nationwide, based in Yonkers, New York.

12 In the absence of action from the federal
13 government, states are beginning to take important
14 steps towards establishing baseline privacy
15 protections.

16 It's crucial, as you've heard from other
17 speakers here today, that any state privacy
18 legislation has strong protections that advance
19 consumer rights, ensure privacy by default, hold
20 companies to real limits on collection sharing and
21 retention, and is backed up by strong enforcements.

22 New privacy protections are needed now more
23 than ever, but this area has been largely
24 unregulated.

25 The biggest tech companies have ballooned

1 into billion-dollar corporations, based on the
2 opaque collection and sharing of consumer data, with
3 few protections or guardrails.

4 There is no general, across-the-board federal
5 privacy law granting consumers baseline protections,
6 and the federal agency tasked with overseeing these
7 companies, the Federal Trade Commission, is vastly
8 underpowered and underresourced.

9 That is why state action is so important and
10 should not be chipped away.

11 States have often led the way in consumer
12 protection.

13 And, later on, those strong protections
14 developed at the state level could be codified by
15 the federal government.

16 Baseline protections, analogous to mandatory
17 seatbelts or air bags, are needed so consumers can
18 safely use apps, social media, and online services
19 without having to compromise their rights to
20 privacy.

21 Consumers want more, not fewer, protections.

22 For example, 92 percent of Americans think
23 that their Internet service provider should provide
24 greater control over the sale of their personal
25 information.

1 More than half of consumers don't trust
2 social-media companies to keep their information
3 safely protected.

4 And almost three-quarters say that it's very
5 important to have control over their information.

6 Recent scandals involving the illicit sharing
7 or sale of personal information have revealed broad
8 unease among consumers about data sharing.

9 Clearly, consumers value their smartphones
10 and their devices and connected products, and other
11 apps and services, but they don't have confidence
12 that their information is being adequately
13 protected.

14 So we at Consumer Reports have been
15 supporting the SHIELD Act to improve information
16 security.

17 We have not taken a position yet on the other
18 two privacy bills that are pending, but we think
19 they have many promising features.

20 On the SHIELD Act, we agree with the attorney
21 general, and many other parties, that this would be
22 a really good law for consumers.

23 We would note that, consumers lost
24 approximately 3.4 billion to new account fraud in
25 2018.

1 And so, in light of the epidemic of data
2 breaches we're seeing across the country, and the
3 lack of broad requirements for information security,
4 we think that's a very important law for New York to
5 pass.

6 With respect to the privacy bills, S5462
7 would provide stronger protections; for example, by
8 requiring the company to obtain permission before
9 collecting, using, or sharing information with
10 another company.

11 It also has appropriately strong enforcement
12 provisions, including the private right of action.

13 So we like that bill.

14 We think it could be strengthened in various
15 ways, in some of the provisions, in addressing some
16 of the definitions.

17 We give one example in our statements.

18 We also like Assemblymember Kim's bill,
19 A7736, which includes privacy provisions that have
20 been recommended by Consumer Reports, including data
21 minimization and affirmative consent to additional
22 collection and sharing, restrictions on charging
23 consumers more for declining to sell their data to
24 third parties, and strong enforcement provisions.

25 So we look forward to working with New York

1 legislators on privacy legislation.

2 We really thank you for your attention to it
3 here, and look forward to working with you going
4 forward.

5 SENATOR SAVINO: (Microphone turned off.)

6 Thank you, both.

7 So, so far, the first two panels like the
8 SHIELD Act; split evenly on the New York Privacy
9 Act.

10 (Microphone turned on.)

11 You two seem to be a little bit of both.

12 And I know Senator Thomas has a lot of
13 questions for you, but I have one question about the
14 other states.

15 You said, "Lessons from other states" --

16 And it made me think of something.

17 -- "comprehensive privacy legislation must
18 reach more than just sales."

19 So you mentioned in the testimony that:

20 "Legislation that focuses solely or primarily
21 on the sale of personal information, as California's
22 law does, misses the mark.

23 "Many entities that profit off of personal
24 information do not sell that information; rather,
25 they leverage it to sell advertisements.

1 "An advertiser approach is an entity with an
2 audience it would like to reach, say, suburban women
3 with children who drive mini vans and like the color
4 blue, and the entity uses the personal information."

5 So it made me think about the use of digital
6 ads in political campaigns.

7 We all do it.

8 So how would we -- how would -- as people who
9 are developing a policy or a statute, how do we do
10 it in a way that we're also cognizant that we're
11 buying and selling people's data for the purposes of
12 advancing political campaigns?

13 ALLIE BOHM: Sure.

14 And so I think it depends on what your
15 construct is. Right?

16 There's certainly, sort of, constitutionally,
17 I think, based on Sorell, you'd have a lot of
18 trouble carving out political ads.

19 Right?

20 That that would have serious First Amendment
21 problems.

22 But, if you're not looking at a ban on
23 targeted advertising; rather, you're looking at, you
24 know, I think CDT would probably say, restrictions
25 on what, you know, personal data can be used.

1 We actually haven't -- at the NYCLU, have not
2 abandoned the idea of meaningful notice and choice.

3 We think the way it's now is not meaningful.

4 We think, you know, the 40-page privacy
5 policy in size 8 font doesn't provide anybody with
6 notice.

7 And the choice that says, you know, Click
8 here to say okay, or you can't use our website, is
9 not a choice.

10 But if you did have a regime that figured out
11 how to meaningfully tell the people the information
12 they need to know about what -- you know, and give
13 them real choices about what their data could be
14 collected and used for, people might opt in to
15 targeted advertising.

16 I've certainly heard people give very, very
17 passionate defenses of targeted advertising.

18 And, in that case, data would be able to be
19 used for targeted advertising for your political
20 ads.

21 I think you're also going to continue to see
22 contextual advertising.

23 You know, I don't think any of the proposals
24 would get rid of advertising based on, so I'm
25 searching for, you know, senators running for

1 reelection in New York. You know, that might be a
2 time that your ad pops up.

3 Or, even, I'm on searching for issues that
4 you were particularly passionate about, that might
5 be a time that your ad pops up.

6 Or you happen to know that folks who read
7 "The New York Times" are likely to be Democratic
8 voters.

9 I don't want to (indiscernible) Republicans
10 should read "The New York Times" too. I don't want
11 to say that that's a thing.

12 You know, maybe that's where you place your
13 ad.

14 And the data are pretty mixed as to whether
15 contextual advertising is, in fact, as effective, or
16 even more effective, than targeted advertising.

17 SENATOR SAVINO: Hmm. Interesting.

18 Thank you.

19 I'll hand it over to the sponsor of the bill.

20 SENATOR THOMAS: I don't have too many
21 questions, but what I want to touch on is, you know,
22 we've talked about personal information, and what,
23 you know, these data companies have on us, and how
24 they use it to discriminate, how they use it to
25 target us with advertisements.

1 How would you define "personal information"?

2 ALLIE BOHM: Sure.

3 So much like my colleagues on the previous
4 panel, I'd like to see a definition that's pretty
5 broad, that talks about information that is
6 reasonably linkable, directly or indirectly, to a
7 specific individual, household, or device.

8 And, you know, part of the reason for that
9 is, you know, as our colleagues talked about, so
10 much of the nefarious practices, that I talked about
11 in my opening statement, operate not just because
12 someone knows that they're targeting you,
13 Senator Thomas, but because somebody knows that
14 they're targeting a device that has this
15 constellation of interests and activities it's
16 engaged in.

17 Your identity doesn't really matter.

18 I want to put a finer point, and I want to
19 articulate a space where I think we differ from CDT,
20 and that is, we really don't feel -- and
21 I appreciate the fact that your bill does not
22 perpetuate what's called the
23 "sensitive/non-sensitive distinction," and that's a
24 distinction that provides greater protections for
25 so-called "sensitive information," things like your

1 first and last name or your Social Security number,
2 and then for other information.

3 And that's because so-called "non-sensitive
4 information," often in the aggregate, and sometimes
5 individually, can, in fact, reveal very sensitive
6 information.

7 So if I'm -- my shopping history is usually
8 not sensitive.

9 My health history is.

10 If I'm shopping at Head Covers Unlimited or
11 TLC Direct, those are both websites that specialize
12 in hats for cancer patients.

13 It's probably trivial to infer my health
14 status.

15 Also, different people view different pieces
16 of information, sensitivity levels, differently.

17 So we really feel like this broad
18 definition -- and you do this really well in your
19 bill -- is super important, to make sure that we're
20 capturing all of the ways that data can be used,
21 frankly, to discriminate against us.

22 CHARLES BELL: If I could just add, I think
23 there's a concern for consumers that we have lost
24 all control over the information that companies have
25 about us, and that they collect things that are

1 barely on the fringes of our awareness that could
2 even be collected.

3 So one example I would give of that, is that
4 some fintech companies, apparently, collect the
5 speed with which you fill out an application on your
6 smartphone or tablet, and use that information in
7 evaluating your worthiness for a loan or for
8 granting credit.

9 So the consumer doesn't necessarily know that
10 that information exists.

11 Perhaps they weren't filling out the loan --
12 the application as quickly as they might, because
13 they were juggling with their other hand, or perhaps
14 they have a disability.

15 And so a company might acquire a piece of
16 information like that, and retain it for a very long
17 period, with no ability for the consumer to review
18 or correct it.

19 And so under the Fair Credit Reporting Act we
20 have certain protections. We're supposed to be able
21 to protect information supplied by creditors about
22 debts that we owe or bills that we didn't pay.

23 And that process has actually proved to be
24 exceedingly difficult for consumers, with over half
25 of consumers giving up because they find it almost

1 impossible to get satisfaction.

2 So my point is that, there's all kinds of
3 data that's being retained by companies. Consumers
4 are not aware of the broad range of things that data
5 brokers and other companies have on them. And it --
6 some of it may well be erroneous, and yet it's
7 getting swept into the big data universe, and can be
8 used in the algorithmic processes to decide what
9 consumers get and what price they're going to pay.

10 And so, that, I think we have to look at this
11 question in that light.

12 SENATOR THOMAS: Allie, since you're with the
13 NYCLU, do you know of any cases that have been
14 brought when it's been discovered that a consumer
15 has been discriminated against, whether it be prices
16 or, like, you know, a job going away or a promotion
17 not being handed down?

18 Have you -- do you know of any cases like
19 that?

20 ALLIE BOHM: Sure.

21 So my colleagues at ACLU National, along with
22 several litigators at other law firms and
23 organizations, recently settled a case with Facebook
24 over discriminatory advertising practices.

25 And because Facebook's advertising platform

1 allowed folks -- or, I'm sorry, allowed advertisers
2 to make selections, either based on, you know,
3 finding look-alike audiences for their existing
4 list, or, you know, narrowing by particular
5 ZIP codes, or, just picking categories that were
6 really likely to be proxies for sex or race or age.

7 There were -- women were not seeing job
8 postings. Older workers were not seeing job
9 postings. African-Americans were not seeing housing
10 ads.

11 And that case settled, and Facebook agreed to
12 create a separate advertising platform -- I should
13 say, that cluster of cases, ACLU's was one of them,
14 settled, and Facebook agreed to create a separate
15 advertising platform for housing, credit issuing,
16 and employment ads, I believe those were the three
17 categories, where there would not be -- everything
18 would have to be a 20-mile radius from a point
19 specific; so either the specific, you know, center
20 of the city or, you know, a particular address, so
21 you couldn't do some of the, you know, redlining.

22 And then, also, taking out a lot of those
23 proxies that were being used for sex, race, and age.

24 SENATOR THOMAS: Do you see a lot of lawsuits
25 based off of this?

1 ALLIE BOHM: I -- you know, to be perfectly
2 honest with you, I haven't been following it as
3 closely as I wished that I could have.

4 But I'd be happy to follow up with your
5 office with that information.

6 SENATOR THOMAS: The first panel had
7 expressed their displeasure to the private right of
8 action, and how that would increase the number of
9 lawsuits.

10 That was one of the reasons why I asked you
11 that question, you know, how many have you seen?

12 Do you think that, because there's a private
13 right of action here, there will be a tendency for
14 abuse?

15 So if you want to comment on that.

16 ALLIE BOHM: Sure.

17 You know, I think the last panel answered
18 this really well.

19 Lawyers generally don't want to bring
20 frivolous lawsuits, right, and, so, to the extent
21 that lawyers, because you can be sanctioned, or,
22 because you're going to lose, and then you're not
23 going to get your attorney's fees. Right?

24 So, you know, I do think that is a check.

25 I think we will see more lawsuits.

1 And there have been a number of lawsuits
2 under Illinois' Biometric Privacy Act.

3 There's good reason for that.

4 You know, part of this is checking really,
5 really problematic behavior on the part of
6 companies.

7 And, you know, right now, all of the costs
8 that come from data breaches or misuse of personal
9 information, all of the costs that I outlined in my
10 opening statement, are being borne by consumers.

11 In some cases, and, you know, your "data
12 fiduciary" idea gets at this, the least-cost avoider
13 is actually the company.

14 Right?

15 They're the ones who understand what data
16 they're collecting, what security measures they're
17 using, what the state of the industry is, where --
18 how exactly they're advertising, what they're using
19 data for, who they're sharing it with.

20 And they're going to be in the better place
21 to avoid harm, to use a very, very broad term.

22 And the way to incentivize them to do that,
23 is to make the cost associated with every time they
24 screw up, higher.

25 Right now that cost is really low.

1 You know, we just heard the previous panel
2 say, you know, California thinks their AG's office
3 can only bring three lawsuits a year.

4 We know the FTC only steps in for the most
5 egregious violations.

6 And that makes sense as a, you know, sort of
7 limited use of federal resources.

8 We need the private right of action for folks
9 to step in and vindicate their own rights when, you
10 know, maybe the breach or the harm was small enough
11 that the New York's AG's office isn't going to feel
12 that it's a good use of their resources to step in.

13 SENATOR THOMAS: The fiduciary -- the data
14 fiduciary in my bill, industry basically is saying,
15 hey, we can't balance both a duty of loyalty to the
16 consumer and a duty of loyalty to the shareholder.

17 Do you have some comments on that?

18 ALLIE BOHM: Well, your bill handles that
19 very well, because your bill explicitly provides
20 that the duty to the user, whose information is
21 being obtained, comes before the duty to the
22 shareholder.

23 CHARLES BELL: You know, I would have to
24 respond to that one in writing.

25 I think for us it's a little bit more of a

1 complicated position.

2 We think that companies should show respect
3 for their customers.

4 I think we have some concerns about the
5 practicality of implementing fiduciary standards for
6 this purpose.

7 But, I would love to consult my brain trust
8 in D.C. and California, and send you some comments
9 on that.

10 SENATOR THOMAS: Fine, will do.

11 Thank you so much, both of you.

12 Third panel, dismissed.

13 CHARLES BELL: Thank you.

14 ALLIE BOHM: Thank you.

15 SENATOR THOMAS: All right, so we have the
16 fourth panel here.

17 This is the New York State Attorney General's
18 Office, with Kate Powers.

19 And you are...?

20 KATE POWERS: This is Cassie Walker, who is
21 also with the office.

22 She won't be testifying.

23 SENATOR THOMAS: Of course.

24 And will you be taking questions, or, no,
25 you're just going to read the statement?

1 KATE POWERS: We won't be taking questions.
2 If you have questions, we would be happy to
3 follow up with you after the hearing.

4 SENATOR THOMAS: Will do, that's great.
5 You may start, whenever.

6 KATE POWERS: So, good afternoon,
7 Chairs Thomas and Savino.

8 My name is Kate Powers. I'm with the office
9 of legislative affairs at the New York Attorney
10 General's Office.

11 I will be reading the testimony of
12 Clark Russell, who could not be here today.

13 Clark is the deputy bureau chief of the
14 bureau on internet and technology, and he oversees
15 the data-breach notification program, and all
16 investigations conducted by the attorney general's
17 office into data breaches affecting New Yorkers.

18 "More than ever, our way of life relies on
19 electronic data.

20 "Indeed, almost every business transaction
21 and communication involves electronic data.

22 "This information has value to wrongdoers,
23 and has led to an explosion in the number of data
24 breaches.

25 "We are losing the war.

1 "So, in light of that, we would like to thank
2 you for the opportunity today to provide testimony
3 in support of the Stop Hacks and Improve Electronic
4 Data Security Act (the SHIELD Act)?

5 "In 2006, the attorney general's office
6 received 300 data-breach notifications.

7 "In 2018, the office received over
8 1400 data-breach notifications.

9 "In the interim, we experienced data breaches
10 involving tens of millions of records at companies
11 like Home Depot, TJX, Uber, and Anthem, and hundreds
12 of millions of records at companies like Yahoo!,
13 Equifax, Marriott, eBay, and Target.

14 "The main cause of this explosion of data
15 breaches is hacking, followed by employee
16 negligence.

17 "Under current law, companies can compile
18 troves of sensitive data about individual
19 New Yorkers, but there is no black letter law
20 requiring reasonable data security to protect this
21 information unless the company is in a specific
22 industry.

23 "Under current law, a company does not need
24 to notify you if your online credentials or your
25 biometric data gets disclosed to an identity thief.

1 "The Stop Hacks and Improve Electronic Data
2 Security Act (the SHIELD Act) seeks to update the
3 law, consistent with what many other states have
4 already done.

5 "First, the SHIELD Act expands the types of
6 data that trigger reporting requirements to include
7 user name and password combinations, biometric data,
8 and HIPPA-covered data.

9 "If the company already had to provide notice
10 to consumers pursuant to another federal or state
11 regulatory scheme, they do not need to provide a
12 second notice under our bill.

13 "It also implies" -- "applies when
14 unauthorized third parties have access to the
15 information, in addition to the current trigger for
16 acquisition.

17 "This is important, because our experience
18 investigating these types of breaches has shown us
19 that, oftentimes, log files or other relevant
20 electronic evidence necessary to prove acquisition
21 of the private information is unavailable despite
22 the fact that a breach occurred.

23 "The SHIELD Act also requires companies to
24 adopt reasonable administrative, technical, and
25 physical safeguards to protect private information.

1 "The standards would apply to any business
2 that holds sensitive data of New Yorkers whether
3 they do business in New York or not.

4 "The reasonable standard of care is in most
5 all data security laws at the state and federal
6 level, and provides a standard that is flexible. It
7 can be adapted to changes in technology, sensitivity
8 of the data retained, and the size and complexity of
9 the business.

10 "The bill's flexibility is also evidenced by
11 its carve-out of compliant regulated entities,
12 defined as "those already regulated by existing or
13 future data-breach regulations of any federal or
14 New York State government entity, including the
15 State Department of Financial Services' regulations,
16 regulations under Gramm-Leach-Bliley, and HIPPA
17 regulations," by deeming them compliant with the
18 law's reasonable security requirement if the entity
19 is compliant with their industry's regulations.

20 "Unfortunately, when a breach occurs,
21 consumers often have limited options.

22 "Credit monitoring helps consumers identify
23 suspicious transactions, but it only alerts the
24 consumer after someone has already stolen her
25 identity.

1 "Credit freezes stop wrongdoers from opening
2 a line of credit in a consumer's name, but a thief
3 can still file for government benefits in the
4 consumer's name or file a fraudulent tax return.

5 "Of course consumers need to stay vigilant.

6 "They should create strong passwords for
7 online accounts and use different passwords for
8 differing accounts.

9 "In addition, to avoid computer viruses and
10 online scams, they should avoid opening suspicious
11 e-mail or clicking on suspicious hyperlinks.

12 "But the fact is, the best way to address the
13 issue is to stop breaches before they happen.

14 "Businesses should only collect the
15 information they need to conduct their business, and
16 securely delete and destroy it when it is no longer
17 needed.

18 "They should design and implement an
19 information security plan, they should designate a
20 person responsible for the plan, and educate and
21 train their employees.

22 "Finally, they should continually review
23 their plan and revise it as new threats emerge or
24 their business changes.

25 "The Committee, and the Legislature in

1 general, has an important opportunity to address
2 what is a defining issue of our time.

3 "By updating New York's data security, we can
4 provide the protection that consumers need and
5 deserve.

6 "We propose the SHIELD Act because we believe
7 it is essential to help to addressing the threats
8 posed by hackers and data breaches.

9 "We thank both of the Chairs for convening
10 this important hearing, and we urge the Senate to
11 pass the SHIELD Act before the end of this
12 legislative session.

13 "Thank you."

14 SENATOR THOMAS: Thank you.

15 All right, can we have Panel 5, and the last
16 one.

17 We're just going to wait for Marta to return
18 before we start. All right?

19 (A recess commences.)

20 (The public hearing resumes.)

21 SENATOR THOMAS: All right, let's get started
22 on our last panel here, Panel 5.

23 Again, forgive me if I slaughter anyone's
24 name.

25 From DLA Piper, LLC, we have Andrew Kingman;

1 From the Business Council of New York State,
2 we have John Evers;

3 From Ropes & Gray, we have Marta Belcher;

4 And from Soramitsu Company, we have
5 James Loperfido.

6 All right.

7 So again, the rules:

8 20 minutes for the entire panel; so 5 minutes
9 each.

10 Summarize your testimony. You don't have to
11 read through it. We have it right here.

12 Our attention span is pretty off right now.

13 [Laughter.]

14 SENATOR THOMAS: So just keep it short, all
15 right, guys?

16 Let's go.

17 JAMES LOPERFIDO: Is this thing on?

18 SENATOR THOMAS: Yes.

19 JAMES LOPERFIDO: Good, all right.

20 At the risk of sounding original after all
21 the other testimony, and having less time than we
22 originally thought, I'll try and abbreviate the best
23 that I can.

24 Thanks for the opportunity to come.

25 Happy to share testimony relating to the

1 bills proposed.

2 My names is James Loperfido, a proud native
3 resident of New York City, and I serve as the
4 vice president of business development for
5 Soramitsu, which is a global Japanese technology
6 consulting company, with a global footprint that
7 specializes in real-world applications of blockchain
8 technology.

9 We're a member of the Hyperledger Group, a
10 consortium of open-sourced blockchain solutions,
11 endorsed by the Linux Foundation, which means we
12 have nothing to hide.

13 My more valuable feedback will likely pertain
14 to Bill 5642, the New York Privacy Act, as a
15 generalist in the technology startup space.

16 So I'll speak to that now.

17 According to Domo's "Data Never Sleeps"
18 report, we create 2.5 quintillion bytes of data
19 every day.

20 With estimated growth figures, we'll
21 produce about one high-quality picture's worth, or,
22 1.7 megabytes of data per second, per person on this
23 planet, by the year 2020.

24 So the enormity of this problem is only
25 growing in scale.

1 The importance of authenticity and providence
2 of data, especially as it relates to an individual's
3 digital identity, must be deliberately understood,
4 managed, and protected.

5 The confluence of powerful technologies,
6 including 5G, satellite Internet networks,
7 artificial intelligence, the Internet of things,
8 cryptocurrencies, and other technological
9 innovations, will create a further explosion of
10 data, both authentic and purposely deceptive.

11 Data pertaining to our individual likeness
12 has specific value, and today that information is
13 exchanged in a relatively opaque fashion for
14 significant amounts of money.

15 That value persists after data change hand
16 the first time, and we as individuals must be
17 perennial stewards of our own to ensure its
18 integrity and utility.

19 Ensuring we have unlimited knowledge with
20 respect to how our data is shared, which our bill
21 seeks to address; who it is shared with, and why, is
22 crucial.

23 Much like the idea that 800 million to
24 2 trillion dollars a year is laundered each year
25 around the world, we cannot possibly begin to

1 estimate with any degree of confidence how much of
2 our personal data is misappropriated and potentially
3 used against us.

4 According to Javelin Strategy and Research,
5 there was 16.7 million victims of identity theft in
6 2017, resulting in \$16.8 billion of fraud.

7 The question of data ownership and
8 maintenance becomes a focal point amidst burgeoning
9 technologies which creates some premise -- or,
10 promise to correct our course.

11 The burden of proof, though, is a grand one
12 for those fiduciaries responsible for our consumer
13 data.

14 Data are extremely portable by their nature,
15 either physically through hardware or virtually
16 through shared access to a common database.

17 Both possibilities generally preclude
18 auditability with a high degree of certainty,
19 regarding that the data in question and its
20 parent -- and their apparent security.

21 Accordingly, permanently relinquishing access
22 to valuable personal data from the ether of the
23 Internet becomes a very tricky task to both execute,
24 monitor, or enforce.

25 Because of social-media platforms like

1 Facebook, credit services like Equifax, and index
2 engines like Google, our digital identity and
3 associated data points relegated to each of us
4 remain visible to many.

5 The centralization of stewardship creates a
6 power dynamic we have yet to comprehend the
7 potential of.

8 The potentiality of decentralization,
9 however, creates an entirely new paradigm to which
10 we must pay attention.

11 How does a custodian or controller, according
12 to the definitions in these bills, of personal data
13 prove to the rest of the world that the data itself
14 is secure and shared only with those who have been
15 granted permission to access it?

16 How can we be sure that de-identified data
17 are as such as, and remain so?

18 Can we guarantee that this de-identified data
19 will remain decoupled from personally identifiable
20 information if needed to be?

21 In an increasingly connected world, security,
22 authenticity, and use of personal data are matters
23 of both personal and national security.

24 To protect New Yorkers' and Americans' data,
25 we must acknowledge that the nature of this value

1 exchange is global.

2 We must work hard to prevent the individual
3 in a global, social, and economic framework from
4 becoming just another statistic.

5 The Senate bills in question are a great
6 start to shaping the standards required for
7 transparent custody and transmission of personal
8 data, but just begin to scratch the surface on the
9 path to harnessing and fostering technological
10 growth.

11 I implore the Committee members to --
12 responsible here to question the essence of data
13 ownership, digital identity, and the impact their
14 evolution has on the real world, especially with
15 respect to a globalized economy.

16 Frontier technologies pose threats, but also
17 creative and powerful solutions to concerns of data
18 privacy.

19 Proactively creating a functional, ethical,
20 and legal framework through careful promotion of
21 their positive attributes, before rampant
22 proliferation, is prudent.

23 I'm happy to speak to my understanding of
24 blockchain technology, its relevance to digital
25 identity, and the problems it has the potential to

1 solve to the best of my ability, and look forward to
2 your questions.

3 Thank you.

4 SENATOR THOMAS: Marta.

5 MARTA BELCHER: Thank you very much for
6 having me, to testify about the potential impact of
7 these privacy bills on the blockchain industry.

8 So building on what James has said, I think
9 there are two things that the New York State
10 Legislature should take into account, with regards
11 to blockchain technology, in forming this privacy
12 legislation.

13 The first thing is that, blockchain actually
14 has -- is very much in line with the ideals of this
15 privacy legislation.

16 And building what on James said, there are a
17 lot of potential applications for blockchain
18 technology that actually can help with users,
19 allowing them to control and own their data in a way
20 they never have been able to before, and I'll give
21 you some examples of that.

22 But, because of that, it's important that
23 this legislation does not render blockchain
24 technology to be automatically non-compliant, which
25 is the concern here.

1 And -- so to give you some examples,
2 I explained in my written testimony, and won't
3 repeat here, sort of a -- a sort of basic
4 Blockchain 101.

5 But I want to give you an example of how you
6 can imagine blockchain technology helping users own
7 their data.

8 So one of the things I talk about in my
9 written testimony is the ability of smart contracts;
10 being able to program your money.

11 So you could program your money to say, for
12 example, for every second of a song that's playing,
13 automatically transfer 1 one-millionth of a cent to
14 the songwriter.

15 And one thing you can do with regards to
16 data, is actually store data on a blockchain, along
17 with permissions on who can use that data, for what.

18 So, for example, I could say:

19 Here's my health data.

20 Please store this on a blockchain with
21 permissions that say, genomics -- you can use this
22 for a genomics researcher.

23 A genomics researcher can use this, but the,
24 you know, advertising industry can't.

25 Right?

1 And that could be -- that data could be
2 tracked as it goes from party to party with those
3 permissions continuing on.

4 And you could even program it to say, every
5 time that any party uses this data for one of the
6 things I've said they can use it for, they actually
7 are going to automatically transfer me
8 1 one-millionth of a cent, right, without ever
9 having to have an intermediary involved.

10 That's something I talk about.

11 And the ideals, of course, of blockchain and
12 cryptocurrency are really in line with the ideals of
13 privacy.

14 So as a result, I want to talk a little bit
15 about the potential issues with these bills.

16 So the things that actually make blockchains
17 so powerful and important are its decentralization
18 and its immutability, but that actually creates some
19 tension with this privacy legislation.

20 This was actually observed, sort of
21 extensively, with the GDPR, which, of course, this
22 legislation was actually, you know, based in part
23 on.

24 And the first issue is that it really assumes
25 a centralized data-governance model, whereas, as

1 I explain in my testimony, blockchain is actually
2 decentralized.

3 So if you're looking, for example, to figure
4 out who a processor or controller is, right, how
5 does that work in a decentralized model where there
6 isn't necessarily one person making the decisions;
7 but, rather, it's spread out among all of the users?

8 Who then has that processor liability?

9 And how do you -- how do you, you know, take
10 on that liability as just a regular user?

11 And then the biggest issue is really with the
12 fact that the whole point of a blockchain, is that
13 you have recorded the -- you have recorded the
14 information permanently, forever. It cannot be
15 deleted.

16 And, of course, one of the things in these
17 bills is a requirement that you actually delete
18 data.

19 And so that sort of fundamentally renders
20 blockchain, potentially, non-compliant, without
21 taking really special care to make sure that the
22 language in the bills does not impose undue
23 requirements on the blockchain industry that they
24 simply can't comply with.

25 So, in short, and in summary, I think

1 blockchain is really, not a magic wand, but has a
2 lot of, potentially, exciting applications,
3 including applications in furthering the goals of
4 this privacy legislation.

5 And as a result, I think it's very important
6 to make sure that this legislation doesn't have the
7 unintended consequence of stifling blockchain
8 innovation in New York.

9 JOHN T. EVERS, Ph.D.: Chairman Thomas,
10 Chairwoman Savino, I want to thank you for this
11 opportunity.

12 My name is John Evers. I'm director of
13 government affairs for the Business Counsel of
14 New York State, the largest employer association in
15 the state.

16 My comments are largely on the SHIELD Act, so
17 let me say at the outset that we think it's not a
18 perfect bill, but as in all things that are rapidly
19 changing and advancing, it's a good start.

20 In fact, this bill has been the subject of
21 well over two years of discussions, conferences, and
22 negotiations between the business council and the
23 office of the attorney general, and we're very
24 pleased that, recently, Assemblyman DenDekker and
25 Senator Thomas accepted amendments for this bill.

1 This legislation provides workable baseline
2 standards for both security features and
3 notification practices for New York State
4 businesses.

5 Importantly, it recognizes existing standards
6 that are universal for businesses nationwide, with
7 clear reporting mechanisms that are largely already
8 in place and best suited to protect the consumer.

9 Federal guidelines, as well as universal
10 state standards, such as recent reporting
11 regulations by DFS, are recognized and accommodated
12 in this law.

13 This would avoid confusion that would be
14 caused by having businesses and/or sectors being
15 subject to multiple standards, an outcome that will
16 only serve to complicate the system with no new
17 discernible benefits to consumers.

18 This bill places into General Business Law
19 and State Technology Law several provisions to stop
20 hacks and improve electronic data security; its
21 name.

22 First: The bill explains the
23 interconnectivity of personal information and
24 private information, and the use of this identifying
25 information in conjunction with financial

1 biometrical information, except passwords,
2 et cetera., to access and acquire personal data.

3 Second: The bill delineates the differences
4 between internal, inadvertent breaches of private
5 data, and external access and acquisition of the
6 data.

7 In the case of the former, an inadvertent
8 breach can be addressed as an incident of which data
9 is accessed internally by those who should not be
10 viewing the data, but no adverse impact has been
11 caused, nor any evidence of malicious intent is
12 found.

13 In these cases, the incident must be reported
14 to the attorney general in writing, and the records
15 maintained for five years.

16 One key provision in the bill is the adoption
17 of new data security protections under a new
18 Section 899-bb of the General Business Law, that
19 places into state law the acceptance of existing
20 federal and state security provisions.

21 These include, as the attorney general's
22 staff just mentioned, Gramm-Leach-Bliley, HIPPA, and
23 also Part 500 of Title 23 of the Official
24 Compilation of Codes, Rules, and Regulations of
25 New York State, and "any other data security and

1 rules and regulations" administered by official
2 departments of the federal and New York State
3 governments.

4 The attorney general review of the cases of
5 breach, and determine what, if any, security
6 practices and systems the entity had been following,
7 and if proper notification procedures were followed.

8 As to "small-business entities," defined as
9 those under 50 employees, or those under certain
10 monetary thresholds, the new guidelines are placed
11 into law.

12 Generally, these are defined, even in the
13 bill, as reasonable.

14 Small businesses must maintain a, quote,
15 data-security program that assures a baseline
16 minimum data security standards, such as training of
17 employees to handle data properly, software and
18 updates that, quote, assess risk in both network and
19 software design.

20 These protective provisions ensure data is
21 accepted, processed, stored, and disposed of
22 properly by small businesses.

23 We are pleased that, under this bill, any
24 action by the attorney general must be brought
25 within three years of the breach, or three years of

1 the attorney general being made aware of the breach,
2 with the statute of limitations being six, except if
3 evidence is found that the breach was hidden.

4 Initial drafts were far too expansive and
5 provided no clear end point as compared to the
6 triggering event.

7 The business council is also pleased that the
8 new version of the bill maintain language, stating,
9 there's no private right of action under this law.

10 We are grateful that this bill, and make it
11 known, this is at least the fourth permutation of
12 this legislation over two years, addresses various
13 parts that we believe would provide work -- that
14 would prove unworkable.

15 As stated above, the bill still contains some
16 provisions that we do not support, such as a
17 doubling, from 10, to 20 dollars, a civil penalty.

18 But it's gratifying that the new law holds
19 government entities to the same standard as those in
20 the private sector, and maintains the exact same
21 baseline data-protection standards for
22 New York State government and agencies, as well as
23 similar reporting mechanisms.

24 And, further, it enlists the help of the
25 office of information technology services to study

1 any breaches, and make recommendations for
2 restoration and improvements to the system.

3 It charges ITS with delivering a report
4 within 90 days on any breach, and mandates ITS
5 develop, quote, regular training to all state
6 entities relating to best practices for the
7 prevention of breach of security of the system.

8 Overall, the business council supports the
9 SHIELD Act.

10 Thank you.

11 SENATOR THOMAS: Thank you.

12 Andrew.

13 ANDREW KINGMAN: Good afternoon.

14 My name is Andrew Kingman.

15 I am here wearing two hats.

16 The first is as a compliance attorney in
17 DLA Piper's cybersecurity and global privacy
18 practice group.

19 I think my firm would ask me to point out
20 that we are an LLP, and not an LLC.

21 [Laughter.]

22 ANDREW KINGMAN: The second is as counsel to
23 the State Privacy and Security Coalition. We're a
24 coalition of 25 retail, media, technology,
25 communications, payment card, and online security

1 companies, as well as six trade associations. And
2 we work on state privacy and cybersecurity
3 legislation nationwide.

4 I also, just to follow up on some of the
5 questions from the prior panels, may be able to help
6 clarify some of the questions around the New York
7 Department of Financial Services' cybersecurity
8 regulations, as well as some of the questions around
9 online political ads and the online ad ecosystem.

10 So we can discuss that perhaps in the
11 question time.

12 I would like to first discuss The SHIELD Act.

13 To echo many of my colleagues, it's something
14 that we also have been working with the
15 attorney general for the last couple of years on.

16 We believe that, overall, it provides
17 sensible updates to New York State's breach law.

18 We work on breach laws nationally.

19 And, so, have offered amendments that would
20 seek to conform this statute to some of the best
21 practices found nationwide.

22 In a data-breach scenario, this is beneficial
23 to the consumer. It increases the efficiency with
24 which consumer notifications can be put together.

25 The greater the uniformity across state lines

1 in requirement, the less time it takes to draft
2 notifications that comply with those requirements.

3 I'd just like to outline, briefly, a couple
4 of the changes that we would like to see.

5 And again, overall, we are supportive of the
6 direction of this bill, and appreciate the
7 Legislature's effort this year. I know it's been
8 the product of several sessions of work.

9 The first would be, to tighten up the
10 "biometrics" definition, and eliminate the clause
11 dealing with "a physical or digital representation."

12 It's not necessarily clear what that would
13 be.

14 It also could implicate things like
15 irreversible hashes of biometric information, which
16 don't pose a security threat to consumers.

17 To answer your question earlier,
18 Senator Thomas, about what the appropriate threshold
19 is for when consumers should receive notification of
20 a data breach, we believe it's, as many states have
21 gone down this path as well, the inclusion of what's
22 called a "harm trigger."

23 So, making sure that consumers are notified
24 when there's a reasonable likelihood -- or, excuse
25 me, a likelihood of harm or identity theft or fraud

1 to that consumer, that that's an appropriate
2 threshold with which to notify consumers,
3 particularly with an access standard, when it's not
4 always clear what information has been acquired;
5 whether a hacker has actually taken that information
6 or not.

7 Allowing an assessment of whether a consumer
8 is subject to some degree of possible harm is an
9 important consideration, and sort of the next step
10 in determining what that type of situation is.

11 So, we detail our rationale for the
12 amendments, but those are two of the main amendments
13 that we would like to further see.

14 But again, supportive, generally, of the
15 direction of this, and appreciate the effort.

16 Many of my colleagues already today have
17 expressed, you know, some of the common concerns
18 around the New York Privacy Act.

19 I'd just like to add a couple of pieces of
20 information there.

21 The first, you know, I think there's been a
22 lot of doubt expressed about the "data fiduciary"
23 standard, for a number of reasons.

24 I think, from a compliance standpoint, it's
25 important, when we're passing very complicated laws

1 that will impact, really, every sector of the
2 New York economy, it's important that businesses be
3 able to build a compliance program around those
4 types of laws.

5 When laws are subject to subjective
6 standards, like some of the issue -- like some of
7 the elements of the privacy harm or privacy risks
8 that are found in the "data fiduciary" standard
9 here, it's impossible to build a compliance program
10 where a business can assess how to deal with the
11 processing of that data.

12 And, so, I think establishing objective
13 standards for -- in requirements is a core component
14 of any privacy legislation.

15 I am not -- you know, our group works on
16 privacy legislation nationally.

17 In over half the states this year, we have
18 seen bills that have attempted to, you know, provide
19 consumer rights or increase privacy protections.

20 We refer to them as "omnibus privacy bills."

21 This is the first bill that has attempted to
22 introduce a "data fiduciary" concept, and so it's
23 not something that has been really considered
24 before, and it's largely academic right now.

25 And I think it's a little bit premature to

1 insert that, particularly coupled with the private
2 right of action, which I'll discuss in a minute
3 here.

4 But, you know, when we're looking at
5 privacy-- okay.

6 SENATOR THOMAS: If you want to quickly
7 summarize.

8 ANDREW KINGMAN: Well, I was just going to
9 say, when we look at privacy legislation, we operate
10 from a framework of three things:

11 One is, ensuring that legislation does
12 increase consumer control and transparency.

13 But with that increased transparency also
14 comes increased cybersecurity threats, because, if a
15 company is making more information public, there are
16 increased vulnerabilities to that.

17 So we want to balance some -- we want to make
18 sure that businesses retain the tools to defend
19 their consumers' information, their employees'
20 information, their company information, from, you
21 know, persistent threats.

22 And then the third piece is operational
23 workability, as I said, making sure that businesses
24 can actually comply with the law in a reasonable
25 way.

1 SENATOR THOMAS: All right, excellent.

2 I'm going to hand this over to
3 Senator Savino.

4 SENATOR SAVINO: Thank you.

5 So I want to focus a bit on the blockchain
6 issue, because, as you know, earlier this year, we
7 passed a blockchain bill in the Senate.

8 I don't think the Assembly has done it yet,
9 but adopting a smart contracts, blockchain, statute.

10 So I'm a little, obviously, interested in how
11 you believe the Senator's proposal will disrupt the
12 blockchain.

13 So if you could explain it a little bit more
14 to me, because my understanding of blockchain, and,
15 believe me, I'm no expert on this, I'm learning as
16 I go, is it --

17 JAMES LOPERFIDO: Nobody is.

18 SENATOR SAVINO: Right, exactly.

19 -- it's not really for the -- to collect
20 data. It's to -- it's transferring it.

21 But nobody really owns the data.

22 It's like it's in little, small pieces,
23 right, it's like a ledger, it's like a digital
24 ledger, so to speak, right, of secure transactions.

25 So in what way would his bill disrupt

1 blockchain?

2 And how could we fix it if we were to amend
3 the language?

4 MARTA BELCHER: Sure, absolutely.

5 So you can actually store, sort of, any
6 length of data on a blockchain.

7 And one thing that the bill talks about, of
8 course, is the definition of, you know, "private
9 information" and "personal data," and what is
10 actually included there.

11 And one thing, that it's really important to
12 clarify, that I think is sort of a gray area right
13 now, is, when data is actually encrypted and stored
14 in an encrypted form, whether that is going to be
15 something that still counts as "personal
16 information" covered by the bill.

17 So one thing that you can do is, basically,
18 create what's called "a hash," which is, basically,
19 a digital fingerprint of data.

20 And I think it's -- that's very important for
21 blockchain technologies, and it's very important to
22 make that clear, that that -- that "a hash" would
23 not count as "personal data" under these bills.

24 SENATOR SAVINO: I see, so there is a
25 potential solutions to this.

1 SENATOR THOMAS: Uh-huh.

2 SENATOR SAVINO: He's whispering behind me
3 (looking over shoulder).

4 JAMES LOPERFIDO: I think there's some
5 misunderstanding, excuse me, with respect to the
6 nature of public blockchain versus the private
7 blockchain, and also the distributed ledger
8 technology, which may or may not include a
9 blockchain necessarily, but, a set of series of
10 distributed ledgers, maintaining a copy of the same
11 information.

12 And adding on to what Marta was saying about,
13 you know, how things are encrypted, and where
14 they're stored, and the idea that some encrypted
15 information can be stored on a server without that
16 server having access to that information.

17 Right?

18 These are very, you know, nitty-gritty
19 concepts, but very important in how data is owned,
20 transferred, and viewed.

21 Right?

22 So within a private permission blockchain,
23 for example, you could store data, and assign both
24 write and read permissions to entities involved in
25 the maintenance and transfer of that data.

1 So -- and, you know, you could very easily
2 preclude public entities, or, whomever, really, from
3 accessing that data.

4 And with respect to a blockchain, yes, it's
5 generally immutable, but there are other versions of
6 distributed-ledger technology, where
7 private-permission scenarios can allow for the
8 actual mutability of data when it's crucial.

9 So there are many -- it's much more of a
10 spectrum than a black-and-white type of thing, is
11 kind of what I'm getting at.

12 SENATOR SAVINO: Thank you.

13 SENATOR THOMAS: So, again, with the
14 blockchain companies, right, this legislation is
15 trying to rein in companies that share and sell
16 information, that uses personal data to target
17 consumers.

18 Are blockchain companies in the business of
19 doing that?

20 JAMES LOPERFIDO: So when I think of private
21 information, I kind of default to Facebook owning
22 most of it, in many ways.

23 And, you know, there's certainly, you know,
24 what I'm seeing in, you know, consumer-facing
25 businesses in the blockchain space, is the potential

1 to disrupt the idea that your data is given away,
2 and that it's then later monetized.

3 You know, and you guys are addressing these
4 ideas.

5 But what I'm seeing is that, there's an
6 incentive, an increasing awareness, that you can own
7 your data and distribute it as you'd like.

8 So, you know, there's definitely the good,
9 bad, and the ugly in the industry, especially with
10 respect to public cryptocurrencies.

11 But, in terms of owning data, and
12 distributing it as needed, on a permission basis,
13 there's a lot of value in that, I think.

14 I don't know if that well answers your
15 question, Senator Thomas, but...

16 SENATOR THOMAS: We're joined by
17 Senator Bailey.

18 To Andrew Kingman, you talked about the data
19 fiduciary, and how it's difficult to comply with the
20 duty of loyalty to the consumer and the duty of
21 loyalty to the board members.

22 Why can't you do both?

23 I mean, I had a panelist that came in
24 earlier, that talked about companies already doing
25 this.

1 You know, when products are created, there's
2 products liability. You know, you're trying to make
3 sure the product doesn't harm the consumer; but at
4 the same time, they have a duty of loyalty to the
5 shareholder.

6 Why can't we do both for data privacy here?

7 ANDREW KINGMAN: Sure.

8 I think -- I think, first of all, there are
9 other ways to ensure that businesses are taking
10 care, and appropriate safeguards, for their customer
11 information.

12 The department of financial services'
13 regulatory regime is one for the cybersecurity
14 requirements.

15 The requirement in the SHIELD Act, that
16 businesses institute reasonable safeguards, is
17 another.

18 In Ohio they passed a bill, providing an
19 affirmative defense for companies that follow
20 well-recognized, like The National Institute of
21 Standards and Technologys' cybersecurity framework,
22 that, following that, and being in reasonable
23 compliance with that, as new additions are released,
24 provides an affirmative defense against enforcement
25 action.

1 So there are lots of ways to incentivize, and
2 to provide more oversight over the way that
3 companies are safeguarding their information.

4 I think a "data fiduciary" standard,
5 particularly one such as this, you know, reading it,
6 and trying to advise a client on how to comply with
7 it, would be very difficult.

8 So, if the question -- just as an example,
9 right, so it would allow: A private right of action
10 by consumers against a company, based on a standard
11 of effects on an individual that are not
12 contemplated by the individual, that are,
13 nevertheless, reasonably foreseeable by the
14 controller assessing the privacy risk that alters
15 the individual's experiences.

16 So, you know, an extreme example of this
17 would be, like a smart refrigerator that regulates
18 power flow, that spoils the milk, that the consumer
19 wasn't expecting that to happen.

20 Does -- does that -- is that grounds for a
21 private right of action?

22 Right?

23 So, these are the types of reasons why it is
24 difficult to implement something that is vague and
25 subjective like that.

1 And I think to the point of the private right
2 of action, which we strongly oppose, you know,
3 Senator Savino, earlier you said that, you know,
4 lawyers only get paid if they win.

5 You know, they also get paid if they settle.

6 Right?

7 And so -- just, you know, I've provided some
8 links in my testimony --

9 SENATOR SAVINO: I think the point I was
10 trying to make is, they don't file cases if they
11 don't have a reasonable expectation they're going to
12 get a settlement out of or win.

13 ANDREW KINGMAN: Well, I cite a couple of
14 studies, actually, in my testimony; one dealing with
15 a study of over 150 class-actions filed federally,
16 and, between 2010 and 2012.

17 And not a single case was resolved on the
18 merits in favor of the plaintiffs.

19 And, you know, it's worth just absorbing that
20 for a minute.

21 31 percent were dismissed by a Court on the
22 merits, and only 33 percent of the cases settled.

23 But more than that, the studies show that
24 what is effective in class-action lawsuits is that
25 it's a transfer of capital from the company to the

1 trial lawyers.

2 Right?

3 So that -- the other statistic that I cite
4 shows that the actual take-home for attorneys,
5 compared to the -- because attorney's fees are based
6 on the total possible number of class-action
7 participants, rather than the people who actually
8 sign up and get the money, that their fees are often
9 300 to 400 percent of the actual take-home of what
10 the consumers are getting.

11 So, to claim that it's a benefit to
12 consumers, or that it provides meaningful recourse
13 for consumers, I don't think that the data actually
14 bears that out.

15 SENATOR THOMAS: A couple of the earlier
16 panelists also talked about First Amendment and
17 commercial-speech rights.

18 What are your thoughts on that?

19 ANDREW KINGMAN: I have fewer thoughts on
20 that. It's not quite in my wheelhouse, so I don't
21 want to get too far over my skis there.

22 SENATOR THOMAS: Okay.

23 ANDREW KINGMAN: I'll let prior panelists'
24 speak -- testimony speak for -- to those points.

25 SENATOR THOMAS: All right.

1 So, thank you all.

2 SENATOR SAVINO: Thank you.

3 SENATOR THOMAS: So I'm going to close out
4 this hearing.

5 I want to thank Senator Savino for sticking
6 by me for a couple of hours.

7 And also Senator Liu for being here to ask
8 questions.

9 And I also want to thank our staff that
10 worked so hard on putting this together, and the
11 panelists that participated today.

12 Like I said at the start of this hearing, we
13 can give New Yorkers their privacy rights and allow
14 our economy to thrive.

15 I'm looking forward to working with all of
16 you to make the lives of consumers better.

17 Thank you so much.

18 (Whereupon, at approximately 1:21 p.m.,
19 the joint committee public hearing concluded, and
20 adjourned.)

21 ---oOo---

22

23

24

25