BEFORE THE NEW YORK STATE SENATE
STANDING COMMITTEE ON CONSUMER PROTECTION
AND
STANDING COMMITTEE ON INTERNET AND TECHNOLOGY

JOINT PUBLIC HEARING:

TO CONDUCT DISCUSSION ON ONLINE PRIVACY,
AND WHAT ROLE THE STATE LEGISLATURE
SHOULD PLAY IN OVERSEEING IT

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

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

PRESIDING:

Senator Kevin Thomas, Chair
Senate Standing Committee on Consumer Protection

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

PRESENT:

Senator John Liu

Senator Jamaal T. Bailey

---oOo---

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

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

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

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

In this modern age we live in data is gold.

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

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

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

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

package or a charge for a service.

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

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

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

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

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

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

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

These are simply unacceptable uses of people's data.

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

That's why we are here today for this

hearing.

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

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

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

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

SENATOR SAVINO: Thank you, Senator Thomas.

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

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

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

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

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

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

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

Thank you.

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

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

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

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

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

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

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

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

Thank you.

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

Forgive me if I slaughter any of your names.

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

We have from TechNET, Christine Fisher;

We have from Tech New York City; Zachary Hecht;

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

All right, so, rules before we start here.

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

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

All right?

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

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

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

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

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

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

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

innovation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

voice our support for S5575, the SHIELD Act.

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

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

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

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

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

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

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

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

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

Some of the negative consequences are:

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

Decreased economic growth for New York;

Increased online security risks;

And chilling effects on free speech and free expression.

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

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

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

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

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

businesses in the United States.

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

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

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

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

OFF-CAMERA SPEAKER: That is time.

JOHN OLSEN: Good morning.

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

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

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

and open Internet.

The Internet creates unprecedented benefits for society.

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

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

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

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

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

I want to first address the proposed New York

Privacy Act, Senate Bill 5642, by Chair Thomas.

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

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

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

The association's primary concerns are as follows:

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

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

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

is being experienced in the European Union under GDPR.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHRISTINA FISHER: Good morning.

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

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

I thank you for the opportunity to testify today.

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

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

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

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

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

First and foremost, is to avoid unintended consequences.

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

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

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

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

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

Startups have little money to invest in compliance.

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

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

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

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

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

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

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

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

Florida or Washington.

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

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

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

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

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

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

Thank you.

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

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

Thank you for the opportunity to be here.

We all shop.

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

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

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

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

We also know that shoppers will walk.

If a retailor mishandles or misuses the data the customers have given freely, they'll lose the business.

In short, retailors use consumer data for the

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

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

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

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

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

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

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

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

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

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

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

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

Among them:

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

Maintain transparency in consumer choice;

Industry neutrality;

Data security of breach notification at the strongest level.

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

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

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

And, not withstanding our opposition as it's currently drafted, we appreciate the opportunity to work with you.

And I know that the retailors that are members of the council will be happy to work

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

So, thank you for the time today.

SENATOR SAVINO: So --

OFF-CAMERA SPEAKER: Two-minute balance.

SENATOR SAVINO: Huh?

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

SENATOR SAVINO: Excellent.

So thank you all.

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

SENATOR SAVINO: Thank you all for your testimony.

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

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

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

But the question I have is:

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

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

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

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

Act, why couldn't everybody do that?

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

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

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

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

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

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

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

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

JOHN OLSEN: Well, I think --

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

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

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

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

person has a legitimate case or not.

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

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

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

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

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

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

But I hear your point on it.

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

Thank you.

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

SENATOR LIU: (Microphone turned off.)

Thank you, Mr. Chair.

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

(Microphone turned on.)

Thank you, Mr. Chair.

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

But I do appreciate this panel's input.

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

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

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

New York.

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

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

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

TED POTRIKUS: I will start with that.

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

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

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

SENATOR LIU: Okay. I mean, just to be

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

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

Maybe some tweaks need to be made here and there?

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

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

JOHN OLSEN: Succinctly, yes.

There is --

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

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

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

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

Americans need an American privacy law.

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

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

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

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

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

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

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

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

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

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

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

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

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

SENATOR LIU: Thank you, Mr. Olsen.

How about the other two experts?

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

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

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

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

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

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

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

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

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

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

And this is very broad.

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

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

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

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

SENATOR LIU: Okay.

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

I appreciate the responses from these individuals.

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

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

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

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

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

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

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

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

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

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

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

SENATOR THOMAS: All right, my turn.

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

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

And you like one, and not the other.

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

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

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

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

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

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

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

perfect strangers, that are sharing one modem.

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

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

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

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

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

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

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

Again, just speaking on the retail-industry side:

Do you get VIP points?

Do you get discounts?

Do you get reduced or free shipping?

Do you get speedier shipping?

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

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

SENATOR THOMAS: The other two experts, any comments?

CHRISTINA FISHER: I would not be able to

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

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

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

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

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

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

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

It makes sense for compliance.

SENATOR THOMAS: From reading the New York

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

Do you have a comment on that?

TED POTRIKUS: I'll officially punt.

I'll get back to you on that one.

SENATOR THOMAS: All right.

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

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

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

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

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

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

It's not simply about cost.

It's really about how the platform functions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Right?

Okay.

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

It's a yes or no.

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

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

But it's --

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

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

Can you expound on that a little bit, when

you're talking about privacy risk?

There's some curious definitions with privacy risk.

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

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

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

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

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

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

Kind of manipulating them in a way.

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

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

JOHN OLSEN: Okay.

I mean, it's a strange approach.

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

Also, what is a consumer willing to give up

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

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

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

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

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

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

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

money.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

challenge.

SENATOR THOMAS: Okay.

I just want to move on to the next question.

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

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

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

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

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

So that's why we support the SHIELD Act.

SENATOR THOMAS: Anyone else?

Same thing?

ZACHARY HECHT: Agreed.

SENATOR THOMAS: Okay.

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

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

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

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

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

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

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

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

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

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

If it's financial information, and you are an

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

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

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

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

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

JOHN OLSEN: Not uniformly.

SENATOR THOMAS: No, not uniformly.

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

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

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

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

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

You know, do you want to enter your password?

Do you want to put in your credit card number?

How much do you want to enter each time?

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

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

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

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

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

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

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

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

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

ZACHARY HECHT: I'm not sure.

I don't think it would.

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

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

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

potentially.

SENATOR THOMAS: Okay.

We're seeing children's privacy being violated.

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

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

Should there be a right to delete?

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

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

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

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

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

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

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

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

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

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

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

So there's already a higher standard there.

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

So that would be, in the case of the

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

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

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

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

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

SENATOR THOMAS: Let's go into targeted advertising.

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

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

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

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

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

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

I don't want this.

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

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

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

SENATOR THOMAS: Anyone else?

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

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

And then there are other personal ad services.

But there is a variety of models out there.

SENATOR THOMAS: Okay.

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

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

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

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

ZACHARY HECHT: So just to echo what I said

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

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

So that's something to also keep in mind.

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

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

SENATOR THOMAS: All right.

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

Do you like anything about my bill?

[Laughter.]

OFF-CAMERA SPEAKER: Say "the sponsor."

ZACHARY HECHT: The sponsor.

SENATOR THOMAS: Oh, thank you, Zach.

You're my favorite now.

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

You know, it's, the devil is in the details.

And it's a common phrase, but it really does mean a lot when it comes to privacy law.

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

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

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

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

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

SENATOR THOMAS: Anyone else?

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

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

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

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

SENATOR THOMAS: Thank you all.

Any questions?

All right.

Panel one is dismissed.

ZACHARY HECHT: Thank you.

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

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

So Panel 2, we have:

From New York Law School, Ari Ezra Waldman.

He's is a professor there, excellent;

Center for Democracy and Technology, we have Joseph Jerome;

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

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

All right, so rules again:

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

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

All right?

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

Go ahead.

ARI EZRA WALDMAN: Great, thank you.

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

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

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

The -- in my written testimony I go into

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

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

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

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

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

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

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

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

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

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

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

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

And that's what "confidentiality" is about.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

And they talked about providing the services for free.

But as we all know, nothing in this world is

free.

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

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

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

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

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

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

LINDSEY BARRETT: Thank you.

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

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

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

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

Second: Privacy rights are civil rights.

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

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

Finally: Characterizing data collectors as

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

I'm mentally surveying what to cut.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

discrimination that data collection can otherwise fuel.

Weak privacy laws also disproportionately disadvantage the poor.

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

It's coercive.

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

Privacy is not just a right to be let alone.

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

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

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

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

Defining data collectors as fiduciaries is a

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

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

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

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

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

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

SENATOR THOMAS: Lindsey --

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

And I'm done.

[Laughter.]

SENATOR THOMAS: All right.

Let's go, Joseph.

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

SENATOR THOMAS: Yeah.

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

My name is Joseph Jerome.

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

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

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

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

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

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

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

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

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

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

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

You asked a question about advertising.

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

Second: Commercial surveillance technologies take advantage of power imbalances.

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

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

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

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

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

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

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

Their recourse is limited.

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

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

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

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

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

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

And New York would not be an outlier here.

The California Consumer Privacy Act is also not an outlier.

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

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

What should a meaningful privacy regulation have?

Let me offer five suggestions.

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

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

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

Geolocation is a good example of this.

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

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

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

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

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

protections.

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

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

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

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

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

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

activities.

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

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

OFF-CAMERA SPEAKER: It's time.

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

SENATOR THOMAS: Mary.

MARY STONE ROSS: (Microphone turned off.)

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

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

My name is Mary Stone Ross.

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

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

OFF-CAMERA SPEAKER: Can you use the microphone?

MARY STONE ROSS: (Microphone turned on.)

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

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

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

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

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

We accomplished this in California.

The CCPA gives all Californians:

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

Second: The right to opt out of the sale;

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

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

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

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

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

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

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

"I'm not a robot."

SENATOR THOMAS: Right.

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

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

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

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

The reporter linked to the Oracle directory.

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

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

Evite is hiding their actual business model

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

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

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

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

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

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

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

advertising.

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

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

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

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

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

I want to conclude with a note of caution.

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

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

SENATOR THOMAS: (Microphone turned off.)

I'll ask the questions.

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

(Microphone turned on.)

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

Did all of you hear what they were talking about?

Okay.

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

MARY STONE ROSS: I can start.

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

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

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

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

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

-- but, there are all of these devices that

are collecting information, and then transmitting it back.

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

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

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

That's by design.

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

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

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

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

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

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

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

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

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

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

and develop personal information.

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

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

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

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

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

Is this a fair concern?

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

their work.

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

There is very little evidence that regulation does stifle innovation.

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

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

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

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

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

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

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

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

[Laughter.]

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

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

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

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

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

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

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

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

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

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

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

Not a whole lot changed.

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

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

have already been doing.

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

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

We keep talking about the brightest flashlight app.

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

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

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

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

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

Innovation.

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

But -- so this is a scary tactic.

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

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

JOSEPH JEROME: Brave.

LINDSEY BARRETT: -- the Brave guy.

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

So it's not impossible.

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

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

phones and the websites that they use?

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

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

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

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

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

It's even more so for kids.

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

There's all kinds of interesting research.

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

think YouTube would collect anything.

You know, they trust it.

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

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

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

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

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

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

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

it.

So you mentioned our Amazon Echo Dot complaint.

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

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

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

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

SENATOR THOMAS: Anyone else?

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

And COPPA is a good law.

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

So any privacy laws should address that, and

make sure that doesn't happen.

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

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

You know, COPPA starts at 13.

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

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

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

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

How long should a company hold personal information?

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

This is the principle of data minimization

and purpose limitation.

And I'd add in privacy by design.

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

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

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

they're going to do.

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

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

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

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

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

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

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

advertising campaigns over a year.

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

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

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

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

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

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

I don't know.

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

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

SENATOR THOMAS: That's true.

Thanks.

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

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

ARI EZRA WALDMAN: No.

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

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

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

between the haves and the have-nots.

I don't think anyone really wants that.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

You mentioned grocery store loyalty programs.

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

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

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

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

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

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

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

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

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

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

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

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

You know, you can get both -- you take

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

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

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

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

Really illuminating.

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

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

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

SENATOR THOMAS: What section is that?

LINDSEY BARRETT: This is a great question.

It might be in my testimony, and I can find that and follow up.

SENATOR THOMAS: Okay. Thank you.

Anyone else?

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

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

That creates a clearer rule for companies.

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

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

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

So, de-identified information is really the

ball game with these laws.

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

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

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

There are three things that I would focus on in terms of potential changes.

One would be, with respect to the "fiduciary" section, to make it a little bit more clear about what the duties of information fiduciaries are.

And I laid those out in my written testimony, as well as discussed it briefly here, duties of care, duties of confidentiality, and duties of loyalty; and describe briefly what that is.

And the Data Care Act does a nice job of that, and there might be a good parallel.

I would also note, just as an aside, that that is not inconsistent with the Delaware corporate law's requirement that companies have fiduciary duties to their shareholders.

There are -- just because a company has a fiduciary duty to their shareholder doesn't mean

that they have other duties.

Products liability, for example, is a really good example. Companies have duties to consumers beyond just duties to their shareholders.

A second thing that I would suggest, that we -- there might -- there's room for a discussion on the role of privacy by design; the idea that privacy should be part of the design process.

I've written quite a bit about this, as well as some others, of what that actually means.

And I think there is a far better way to do it than to just write Article 25, what the GDPR has.

And I talked about that in my written testimony, of a more specific way that companies can -- that provides notice to companies about what "privacy by design" is.

And then, third, I agree with, about the importance of these definitions.

But I also think that we could be even stronger with private rights of action and enforcement.

We shouldn't burden the New York Attorney General's Office with the responsibilities for protecting every element of privacy rights of New York residents.

And there is such a strong capability for private rights of action to have an effect on corporate behavior, that there may be a role for, and I think there is a strong role for, private rights of action for individuals to effect their privacy rights.

MARY STONE ROSS: I have a lot of notes, which I'm happy to share with your office, because they're pretty detailed.

But one thing that I would say, that you got a lot of pushback from the first panel this morning, but, it is critical to say that harm is a privacy injury. That you do not tie it to a market-based harm approach.

That approach is antiquated, and it doesn't work in the privacy context.

And so you already have language in there, which is fantastic, and I commend you for that.

The only thing that I would add is that, in the California law, we allow a third party to opt out on a person's behalf.

And the reason why this is important is, as you can see with that Oracle data directory, there's so many companies out there that are collecting, processing, and selling your personal information,

and an individual has no idea who these companies are.

So it would be great, speaking of another business opportunity, or a non-profit opportunity, to allow other people or organizations to be able to opt out of the sale of your information on your behalf.

SENATOR THOMAS: Thank you.

I'm going to hand this over to Senator Savino now for some questions.

SENATOR SAVINO: (Microphone turned off.)

Thank you.

I'll be brief, because this is complicated, very complicated, but illuminating.

(Microphone turned on.)

And it's almost as if people -- consumers have become willing participants in the loss of their own data, just by virtue of signing up for rewards programs.

I mean, I know I'm guilty of it, we all are, because people like to get things, as you -- I think, Mr. Jerome, you pointed out, that people like their rewards programs.

We all do, because we get something tangible of a benefit.

But it does kind of strike me as weird.

Like, I go into CVS and, you know, you swipe your little card, and they give you this -- you ever go to CVS and you get your receipt, it's like 4 feet long, and it's all the coupons, because they know your buying history.

Everything you've ever bought in the past six months, and they're giving you a coupon for it.

And then the next thing you know, you go home, and you log on, and, suddenly, there's a coupon for that product.

And it is a little frightening.

But more frightening is, I'm looking at this -- on the location service.

So my staff member behind me just gave me her Google locator. And I'm looking at December 15th of -- December 8th of 2015, her entire day.

Even though you can delete some of it, but it's really hard to get rid of this.

Every moment of the day, where she was, what she was doing.

How many minutes she spent driving in a car from her address to Rite Aid.

And going to a college, and then going somewhere else.

That's really scary.

What possible reason could they have to keep all this information for all this time?

Why would they need to know where I was at every moment of a day?

MARY STONE ROSS: I mean, the problem is, right now, why wouldn't they keep all that information?

It's free to hold on to it, and, who knows?

Like, maybe there's some use that they haven't thought of yet to keep it.

So that's why we need regulation, to shift that, so there is some cost to holding on, and collecting all of that information in the first place.

SENATOR SAVINO: I mean, I think, in some respects, there's a value to -- to myself too. Like, sometimes I forget what I was doing.

I go back to my calendar. You know, and as an elected official, it's important, sometimes you need to match up what you did on a particular day, if you're filing your financial disclosure forms or your filing campaign finance forms.

But it never occurred to me that Google locator had my every moment in their system,

somewhere.

MARY STONE ROSS: And, also, that's your calendar, so you should be able to go back and look at it.

But do you want Google and 50 other tracking services, and then, whoever else, to be able to look at that information too.

SENATOR SAVINO: I think the point I'm trying to make is, most people probably have no idea. Right?

So you sign up for, you know, you get a Google account.

You sign up for rewards at CVS or Rite Aid or Macy's, or wherever it is that you do.

You do these things because you think that there's a benefit to you personally, and you get something out of it. You get coupons; you get discounts; you get Macy's books; you get, you know, the 4-foot-long receipt with, you know, extra bucks, or whatever they call it at CVS.

So you get something of value.

But -- so consumers really have no idea that they're doing this.

So -- so how do we -- beyond the passage of this bill and enforcement --

Which I'm not sure how we would do that, that's another challenge.

-- how do we raise awareness among consumers that they need to be more vigilant with their data protection on their own?

ARI EZRA WALDMAN: So it's not just that consumers aren't aware.

And it's -- if consumers were just not aware, then public-awareness campaigns would be effective.

But it's that these processes engage our psycho -- innate psychological barriers to actually understanding it.

Part of the problem is, one of the things we call "hyperbolic discounting."

It's, humans are really, really bad at comparing current benefits, like the loyalty or the discounts that you get from a loyalty program, with the -- with potential future risks.

We just can't adequately balance or assess the risk and reward -- the risk-and-reward basis.

So, given that, then we can't really -- we shouldn't really be focused on giving users more information, or giving them more control, or giving them more choice, because it's a fallacy.

That's what the current law does, and that's

what all transparency laws do, is just to say, give users more information about what's happening.

That's why the structure of laws, like the New York Privacy Act; or laws like, structures of information fiduciaries; or any other -- or privacy by design, are focused on shifting the burden of protecting our privacy from individuals to companies.

So, you ask, how do we help consumers protect their privacy better?

Sure, we can educate, we can put it in curriculum in schools. We can have campaigns about it.

But that's not the goal.

We have to shift the burden to companies, and provide regulation that limits what they can collect, because we are cognitively unable, even with all possible information, to make those adequate choices.

SENATOR SAVINO: Hmm, interesting.

LINDSEY BARRETT: Yeah, I would echo that 1 million percent, and also say that, when we talk about privacy, I think we tend, and I say this, in that, it's become accidental by virtue of very deliberate crafting of, kind of, talking points and

messaging from companies that don't want privacy regulations.

But, we talk about privacy, in terms of consumer protection, in a completely different way than we talk about any other areas of our lives.

Like, we talk about, like, oh, (indiscernible) -- you know, aren't we willing participants, except, oh, by the way, you know, we lack choice. This is in -- you know, it's an area where people aren't able to deal with things.

But we don't say, like, oh, well, you know, you seem perfectly willing to go out and buy spoiled meat.

Like, we don't say, oh, that's what the market will bear.

We say, no, there's a basic line of what people shouldn't be able to subject themselves to.

So I think when we get bogged down too heavily in kind of the willingness and the expectations portion, where, part of it, there's absolutely a grain of truth to it, but there's also an extent to which it blurs the larger truth of the extent to which these aren't, you know, harms that people are able to avoid on their own.

And we talk about privacy in a weirdly, just,

categorically different way than we do other areas of consumer protection.

JOSEPH JEROME: Yeah, I think I'm just echoing what my co-panelists said.

I mean, the reality is, companies are happy to provide us with longer notices and more choices because we are drowning in notices and choices.

And, you know, as a privacy advocate, we have Data Privacy Day once a year, and I'm always called upon to -- by the media and other: What can I do to protect my privacy?

And I'll say something, like, You know, check out all of the apps and privacy settings on your phone.

The average person has 80 apps on their phone.

That's -- even at 5 minutes apiece, how are you going to make the time for that, and we've just handled the phone.

We haven't handled any the smart devices in your home.

We haven't dealt with any of the brick-and-mortar loyalty cards.

We haven't dealt with what employers are doing with your data, what your health companies --

or, insurers are doing with your data.

You mentioned CVS coupons.

I'm always fascinated by what happens when you use your CVS loyalty card at the CVS pharmacy.

We act like we have health privacy laws, but, all of our privacy laws, in general, are very, very leaky, and our health, you know, information falls out of the HIPPA, which is the federal health privacy law, pretty easily.

We spend a lot of time talking about how financial data is very heavily regulated, but the privacy protections around financial data are minimal. You have to go to your bank and see if you can figure out what choices you have about how they share your financial data.

It's easier said than done.

And so I'm just, you know, parroting what both Ari and Lindsey have said.

Individuals can't do the job.

Lawmakers need to start making some decisions (indiscernible cross-talking).

SENATOR SAVINO: Well, truthfully, they mail it, like, they send it to you. Right?

Most of us, we look at it, and then we just toss it because it's, like, 14 pages and it's very

tiny type, and you're just like, ack, and you throw it away.

Yeah, you're right. It's we -- you may be right, we may not be able to cognitively absorb it and internalize it.

MARY STONE ROSS: So one of the ways we addressed this in California is that, if a business is selling personal information, because there is an opt-out, they have to have a button on the button of their page that says, "Do not sell my personal information."

So it's kind of a public shaming.

So AT&T, which you're paying for every month for crappy service, who is also selling your personal information, all of a sudden, when you go to pay your bill, there would be a button on the bottom of the screen that says, "Do not sell my personal information."

And so what we've seen is that, businesses who don't want to -- who don't want to be selling your personal information are making sure that they are compliant, so they don't have that button on the bottom of the screen that actually calls them out on what their business model is, in fact.

SENATOR SAVINO: And does the California law

have a private right of action?

MARY STONE ROSS: No, it got taken out.

It has a private right of action for data breaches, but it got taken out in the legislative compromise.

So this is the problem now.

It's just AG enforcement for most of the law. And their office came out and said, they only think they can only bring three enforcement actions under the CCPA, a year.

But what the initiative had besides the private right of action, is we also allowed district attorneys and city attorneys and city prosecutors to bring action under the law.

SENATOR SAVINO: Have any of them done that?

MARY STONE ROSS: It's not in effect yet.

January 1, 2020.

JOSEPH JEROME: Sorry to interrupt you.

I actually do think more enforcement mechanisms is incredibly important.

And my organization was really involved in the Washington Privacy Act, which had a lot of other really strong ideas, but would have, basically, preempted, again, local, county, and state officials.

And, localities are really playing an important role in the privacy debate.

The Los Angeles Attorney is bringing a lawsuit against the Weather Channel app for, again, selling location data.

We've seen the Washington, D.C., our attorney general, is suing Facebook, pretty successfully so far.

So, again, I think it's important to have avenues of enforcement, and making sure that this isn't just on the attorney -- the state attorney general is vitally important.

LINDSEY BARRETT: And not to mention, Ari mentioned this briefly, but, on the, kind of, private right of action, every time you have an industry panel, they'll say, Oh, my God, you know, we'll be drowning in lawsuits.

But you also think about, kind of, the incentives against people filing lawsuits.

They're expensive, they're difficult.

Most people don't do that.

The way that -- the reason that having a private right of action is important is, one, if there are problems of such a broad scale that it does become, you know, reasonable and meaningful for

someone to pursue that, it's available.

But, also, it says to the companies, no, this is real. You have you to take it seriously. This isn't another privacy law that you can, you know, laugh off because, oh, by the way, you know, the state AG is already swamped, the FTC is swamped, you know, they're not going to do anything about it.

So, in terms of gauging what's actually going to happen, like, the way that having a private right of action shapes incentives is vitally important. And the odds of, you know, having every Tom, Dick, and litigant waltz in and ruining American industry is pretty slim.

SENATOR SAVINO: Uh-huh, that's true.

And we always hear that whenever we're looking to improve people's ability to bring a lawsuit.

Generally, trial attorneys don't take cases unless there's merit to them, because they don't get paid unless they win, so they have to put the effort into it.

But, it's a valid point.

Yes?

MARY STONE ROSS: And just going back to why we had a private right of -- I mean, there's a lot

of reasons why we had a private right of action in the initiative form.

But one of the examples that was really foundational to me, was there's a case going against Facebook right now, that's progressing through the courts, based on an Illinois Biometric Information Privacy Act.

And so Texas actually has a very similar law, but, in Texas, it's only AG enforcement, while, in Illinois, it was AG enforcement, but also a private right of action.

And so we see nothing -- both of these laws have actually been on the books for many, many years.

Texas, nothing happened.

But, in Illinois, they're making quite a bit of progress.

SENATOR SAVINO: Hmm. Very good.

Thank you.

SENATOR THOMAS: All right, thank you all.

Panel 2 is dismissed.

(All panelists say "Thank you.")

SENATOR SAVINO: See, they knew I was talking about them.

My Macy's money is about to expire, they just

sent me. They heard me.

[Laughter.]

SENATOR SAVINO: They heard me.

SENATOR THOMAS: All right.

So we have the third panel here.

Again, if I slaughter anyone's name, please forgive me.

So, from Consumer Reports, we have Charles Bell;

And from the New York Civil Liberties Union, we have Allie Bohm.

So the rules, again, actually, since there are only two of you, you're only going to be given 10 minutes, 5 minutes each.

So, let's start with Allie.

ALLIE BOHM: Thank you for the opportunity to testify today.

My name is Allie Bohm. I'm a policy counsel at the New York Civil Liberties Union.

Oh, that thing moves.

It is no longer possible to participate in society without providing personal information to third parties that may, in and of itself, reveal intimate details of one's life, or, that when combined with other data and analyzed, may expose

such information.

The consequences can be profound.

For example, personal information has been leveraged to ensure that only younger men see certain job postings, and to exclude African-Americans from viewing certain housing advertisements.

Cambridge Analytica obtained more than 50 million Facebook users' personal information, and purported to use that information to convince individuals to vote for Mr. Trump.

During the 2016 election, personal information was also used to target ads to African-Americans, urging them not to vote.

Against this backdrop, the Committee's consideration of online privacy and the state Legislature's role in overseeing it could not be timelier.

Because of the limited time, I will describe the scope of the problem and the legal landscape that any privacy legislation will fall into.

My written statement talks about lessons learned from other -- from our sister states, as well as provides specific feedback on Senator Thomas's New York Privacy Act.

We started our privacy work at the NYCLU by making a list of harms that stem from the pervasive collection, retention, sharing, monetization, use, and misuse of personal information.

Here are some of them.

Entities, whether businesses, employers, schools, landlords, health insurers, or credit-issuing agencies, can use amassed personal information to limit individuals' awareness of and access to opportunities.

Depending on the opportunity, personal information and sophisticated algorithms can be used to circumvent our civil and human rights laws, as I described earlier.

Even when advertisers do not deliberately discriminate, individuals' opportunities may be inadvertently limited as the result of the online advertising industry functioning as intended.

For example, a representative of the Network Advertising Initiative testified at November's Federal Trade Commission hearing that, quote, Women are less likely to see employment ads for careers in the science, technology, engineering, and math field simply because they have higher value to other advertisers because women do more shopping.

In addition, as entities increasingly turn to sophisticated algorithms to place ads, screen resumes, or even in government hands to make bail or child-custody decisions, the training data used to develop the algorithms have outsized impacts on individuals' opportunities and outcomes.

Algorithms work by identifying correlation, not causation, and the training data used to, quote, teach algorithms what patterns to look for, often reflect and magnify entrenched historical biases.

In addition to discrimination based on protected classes, amassed personal information can be used to engage in unfair price discrimination.

Pervasive collection and use of personal information can also exacerbate information disparities and contribute to the erosion of free -- of trust -- (makes verbal sound) -- the erosion of trust and free expression.

I'm trying to go too fast.

Collection and pooling of personal information creates treasure troves for government access. This is because the antiquated third-party doctrine permits the government to get information from third-party custodians without court oversight and without ever telling the individual to whom the

information pertains.

It also creates a bull's eye for data thieves, whether those seeking profit or those seeking to interfere in U.S. elections.

Data breaches, and the misuse of personal information, can lead to financial harm, reputational harm, emotional harm, or physical harm.

It can undermine an individual's job prospects, or family and friend relationships, and can increase the risk of future harms.

Compounding these problems, individuals do not know or consent to the manner in which entities collect, use, retain, share, and monetize their personal information.

Moreover, entities that collect, use, share, retain, and monetize personal information have specialized knowledge about the algorithms and data-security measures they use, as well as about how they collect, use, retain, share, and monetize personal information, that the average individual is unlikely to know or understand.

Still, individuals demonstrate time and again that they care about privacy.

92 percent of Facebook users alter the social network's default privacy settings, indicating that

they wish to choose with whom they share personal information.

Similarly, 92 percent of Americans believe companies should obtain individuals' permission before sharing or selling their personal information.

Drafters seeking to author privacy legislation are not painting on a clean canvas, and any legislation must be crafted to interact well with existing New York and federal sectoral privacy laws.

Moreover, comprehensive privacy legislation must be tailored carefully to comport with Supreme Court precedent.

In Sorrell v. IMS Health, Inc., the Court held, that speaker-based restrictions on the sale, disclosure, and use of personal information to heighten scrutiny, any privacy law that prescribes the collection, use, retention, sharing, or monetization of personal information, based on the purpose for the leveraging or the identity of the entity doing the leveraging, is likely suspect.

The NYCLU appreciates the opportunity to testify today, and apologizes for speeding through this, and stands ready to assist -- to answer any

questions, and also to assist the Committee, Senator Thomas, and other interested lawmakers, as you craft privacy legislation for New York State.

SENATOR THOMAS: Charles.

CHARLES BELL: Chairman Savino, Chairman Thomas, thanks so much for the opportunity to speak today.

My name is Chuck Bell. I'm programs director for Consumer Reports, an independent, non-profit, member organization representing 6 million consumers nationwide, based in Yonkers, New York.

In the absence of action from the federal government, states are beginning to take important steps towards establishing baseline privacy protections.

It's crucial, as you've heard from other speakers here today, that any state privacy legislation has strong protections that advance consumer rights, ensure privacy by default, hold companies to real limits on collection sharing and retention, and is backed up by strong enforcements.

New privacy protections are needed now more than ever, but this area has been largely unregulated.

The biggest tech companies have ballooned

into billion-dollar corporations, based on the opaque collection and sharing of consumer data, with few protections or guardrails.

There is no general, across-the-board federal privacy law granting consumers baseline protections, and the federal agency tasked with overseeing these companies, the Federal Trade Commission, is vastly underpowered and underresourced.

That is why state action is so important and should not be chipped away.

States have often led the way in consumer protection.

And, later on, those strong protections developed at the state level could be codified by the federal government.

Baseline protections, analogous to mandatory seatbelts or air bags, are needed so consumers can safely use apps, social media, and online services without having to compromise their rights to privacy.

Consumers want more, not fewer, protections.

For example, 92 percent of Americans think that their Internet service provider should provide greater control over the sale of their personal information.

More than half of consumers don't trust social-media companies to keep their information safely protected.

And almost three-quarters say that it's very important to have control over their information.

Recent scandals involving the illicit sharing or sale of personal information have revealed broad unease among consumers about data sharing.

Clearly, consumers value their smartphones and their devices and connected products, and other apps and services, but they don't have confidence that their information is being adequately protected.

So we at Consumer Reports have been supporting the SHIELD Act to improve information security.

We have not taken a position yet on the other two privacy bills that are pending, but we think they have many promising features.

On the SHIELD Act, we agree with the attorney general, and many other parties, that this would be a really good law for consumers.

We would note that, consumers lost approximately 3.4 billion to new account fraud in 2018.

And so, in light of the epidemic of data breaches we're seeing across the country, and the lack of broad requirements for information security, we think that's a very important law for New York to pass.

With respect to the privacy bills, S5462 would provide stronger protections; for example, by requiring the company to obtain permission before collecting, using, or sharing information with another company.

It also has appropriately strong enforcement provisions, including the private right of action.

So we like that bill.

We think it could be strengthened in various ways, in some of the provisions, in addressing some of the definitions.

We give one example in our statements.

We also like Assemblymember Kim's bill, A7736, which includes privacy provisions that have been recommended by Consumer Reports, including data minimization and affirmative consent to additional collection and sharing, restrictions on charging consumers more for declining to sell their data to third parties, and strong enforcement provisions.

So we look forward to working with New York

legislators on privacy legislation.

We really thank you for your attention to it here, and look forward to working with you going forward.

SENATOR SAVINO: (Microphone turned off.)

Thank you, both.

So, so far, the first two panels like the SHIELD Act; split evenly on the New York Privacy Act.

(Microphone turned on.)

You two seem to be a little bit of both.

And I know Senator Thomas has a lot of questions for you, but I have one question about the other states.

You said, "Lessons from other states" --

And it made me think of something.

-- "comprehensive privacy legislation must reach more than just sales."

So you mentioned in the testimony that:

"Legislation that focuses solely or primarily on the sale of personal information, as California's law does, misses the mark.

"Many entities that profit off of personal information do not sell that information; rather, they leverage it to sell advertisements.

"An advertiser approach is an entity with an audience it would like to reach, say, suburban women with children who drive mini vans and like the color blue, and the entity uses the personal information."

So it made me think about the use of digital ads in political campaigns.

We all do it.

So how would we -- how would -- as people who are developing a policy or a statute, how do we do it in a way that we're also cognizant that we're buying and selling people's data for the purposes of advancing political campaigns?

ALLIE BOHM: Sure.

And so I think it depends on what your construct is. Right?

There's certainly, sort of, constitutionally, I think, based on Sorell, you'd have a lot of trouble carving out political ads.

Right?

That that would have serious First Amendment problems.

But, if you're not looking at a ban on targeted advertising; rather, you're looking at, you know, I think CDT would probably say, restrictions on what, you know, personal data can be used.

We actually haven't -- at the NYCLU, have not abandoned the idea of meaningful notice and choice.

We think the way it's now is not meaningful.

We think, you know, the 40-page privacy policy in size 8 font doesn't provide anybody with notice.

And the choice that says, you know, Click here to say okay, or you can't use our website, is not a choice.

But if you did have a regime that figured out how to meaningfully tell the people the information they need to know about what -- you know, and give them real choices about what their data could be collected and used for, people might opt in to targeted advertising.

I've certainly heard people give very, very passionate defenses of targeted advertising.

And, in that case, data would be able to be used for targeted advertising for your political ads.

I think you're also going to continue to see contextual advertising.

You know, I don't think any of the proposals would get rid of advertising based on, so I'm searching for, you know, senators running for

reelection in New York. You know, that might be a time that your ad pops up.

Or, even, I'm on searching for issues that you were particularly passionate about, that might be a time that your ad pops up.

Or you happen to know that folks who read "The New York Times" are likely to be Democratic voters.

I don't want to (indiscernible) Republicans should read "The New York Times" too. I don't want to say that that's a thing.

You know, maybe that's where you place your ad.

And the data are pretty mixed as to whether contextual advertising is, in fact, as effective, or even more effective, than targeted advertising.

SENATOR SAVINO: Hmm. Interesting.

Thank you.

I'll hand it over to the sponsor of the bill.

SENATOR THOMAS: I don't have too many questions, but what I want to touch on is, you know, we've talked about personal information, and what, you know, these data companies have on us, and how they use it to discriminate, how they use it to target us with advertisements.

How would you define "personal information"?

ALLIE BOHM: Sure.

So much like my colleagues on the previous panel, I'd like to see a definition that's pretty broad, that talks about information that is reasonably linkable, directly or indirectly, to a specific individual, household, or device.

And, you know, part of the reason for that is, you know, as our colleagues talked about, so much of the nefarious practices, that I talked about in my opening statement, operate not just because someone knows that they're targeting you, Senator Thomas, but because somebody knows that they're targeting a device that has this constellation of interests and activities it's engaged in.

Your identity doesn't really matter.

I want to put a finer point, and I want to articulate a space where I think we differ from CDT, and that is, we really don't feel -- and I appreciate the fact that your bill does not perpetuate what's called the "sensitive/non-sensitive distinction," and that's a distinction that provides greater protections for so-called "sensitive information," things like your

first and last name or your Social Security number, and then for other information.

And that's because so-called "non-sensitive information," often in the aggregate, and sometimes individually, can, in fact, reveal very sensitive information.

So if I'm -- my shopping history is usually not sensitive.

My health history is.

If I'm shopping at Head Covers Unlimited or TLC Direct, those are both websites that specialize in hats for cancer patients.

It's probably trivial to infer my health status.

Also, different people view different pieces of information, sensitivity levels, differently.

So we really feel like this broad definition -- and you do this really well in your bill -- is super important, to make sure that we're capturing all of the ways that data can be used, frankly, to discriminate against us.

CHARLES BELL: If I could just add, I think there's a concern for consumers that we have lost all control over the information that companies have about us, and that they collect things that are

barely on the fringes of our awareness that could even be collected.

So one example I would give of that, is that some fintech companies, apparently, collect the speed with which you fill out an application on your smartphone or tablet, and use that information in evaluating your worthiness for a loan or for granting credit.

So the consumer doesn't necessarily know that that information exists.

Perhaps they weren't filling out the loan -- the application as quickly as they might, because they were juggling with their other hand, or perhaps they have a disability.

And so a company might acquire a piece of information like that, and retain it for a very long period, with no ability for the consumer to review or correct it.

And so under the Fair Credit Reporting Act we have certain protections. We're supposed to be able to protect information supplied by creditors about debts that we owe or bills that we didn't pay.

And that process has actually proved to be exceedingly difficult for consumers, with over half of consumers giving up because they find it almost

impossible to get satisfaction.

So my point is that, there's all kinds of data that's being retained by companies. Consumers are not aware of the broad range of things that data brokers and other companies have on them. And it -- some of it may well be erroneous, and yet it's getting swept into the big data universe, and can be used in the algorithmic processes to decide what consumers get and what price they're going to pay.

And so, that, I think we have to look at this question in that light.

SENATOR THOMAS: Allie, since you're with the NYCLU, do you know of any cases that have been brought when it's been discovered that a consumer has been discriminated against, whether it be prices or, like, you know, a job going away or a promotion not being handed down?

Have you -- do you know of any cases like that?

ALLIE BOHM: Sure.

So my colleagues at ACLU National, along with several litigators at other law firms and organizations, recently settled a case with Facebook over discriminatory advertising practices.

And because Facebook's advertising platform

allowed folks -- or, I'm sorry, allowed advertisers to make selections, either based on, you know, finding look-alike audiences for their existing list, or, you know, narrowing by particular ZIP codes, or, just picking categories that were really likely to be proxies for sex or race or age.

There were -- women were not seeing job postings. Older workers were not seeing job postings. African-Americans were not seeing housing ads.

And that case settled, and Facebook agreed to create a separate advertising platform -- I should say, that cluster of cases, ACLU's was one of them, settled, and Facebook agreed to create a separate advertising platform for housing, credit issuing, and employment ads, I believe those were the three categories, where there would not be -- everything would have to be a 20-mile radius from a point specific; so either the specific, you know, center of the city or, you know, a particular address, so you couldn't do some of the, you know, redlining.

And then, also, taking out a lot of those proxies that were being used for sex, race, and age.

SENATOR THOMAS: Do you see a lot of lawsuits based off of this?

ALLIE BOHM: I -- you know, to be perfectly honest with you, I haven't been following it as closely as I wished that I could have.

But I'd be happy to follow up with your office with that information.

SENATOR THOMAS: The first panel had expressed their displeasure to the private right of action, and how that would increase the number of lawsuits.

That was one of the reasons why I asked you that question, you know, how many have you seen?

Do you think that, because there's a private right of action here, there will be a tendency for abuse?

So if you want to comment on that.

ALLIE BOHM: Sure.

You know, I think the last panel answered this really well.

Lawyers generally don't want to bring frivolous lawsuits, right, and, so, to the extent that lawyers, because you can be sanctioned, or, because you're going to lose, and then you're not going to get your attorney's fees. Right?

So, you know, I do think that is a check.

I think we will see more lawsuits.

And there have been a number of lawsuits under Illinois' Biometric Privacy Act.

There's good reason for that.

You know, part of this is checking really, really problematic behavior on the part of companies.

And, you know, right now, all of the costs that come from data breaches or misuse of personal information, all of the costs that I outlined in my opening statement, are being borne by consumers.

In some cases, and, you know, your "data fiduciary" idea gets at this, the least-cost avoider is actually the company.

Right?

They're the ones who understand what data they're collecting, what security measures they're using, what the state of the industry is, where -- how exactly they're advertising, what they're using data for, who they're sharing it with.

And they're going to be in the better place to avoid harm, to use a very, very broad term.

And the way to incentivize them to do that, is to make the cost associated with every time they screw up, higher.

Right now that cost is really low.

You know, we just heard the previous panel say, you know, California thinks their AG's office can only bring three lawsuits a year.

We know the FTC only steps in for the most egregious violations.

And that makes sense as a, you know, sort of limited use of federal resources.

We need the private right of action for folks to step in and vindicate their own rights when, you know, maybe the breach or the harm was small enough that the New York's AG's office isn't going to feel that it's a good use of their resources to step in.

SENATOR THOMAS: The fiduciary -- the data fiduciary in my bill, industry basically is saying, hey, we can't balance both a duty of loyalty to the consumer and a duty of loyalty to the shareholder.

Do you have some comments on that?

ALLIE BOHM: Well, your bill handles that very well, because your bill explicitly provides that the duty to the user, whose information is being obtained, comes before the duty to the shareholder.

CHARLES BELL: You know, I would have to respond to that one in writing.

I think for us it's a little bit more of a

complicated position.

We think that companies should show respect for their customers.

I think we have some concerns about the practicality of implementing fiduciary standards for this purpose.

But, I would love to consult my brain trust in D.C. and California, and send you some comments on that.

SENATOR THOMAS: Fine, will do.

Thank you so much, both of you.

Third panel, dismissed.

CHARLES BELL: Thank you.

ALLIE BOHM: Thank you.

SENATOR THOMAS: All right, so we have the fourth panel here.

This is the New York State Attorney General's Office, with Kate Powers.

And you are...?

KATE POWERS: This is Cassie Walker, who is also with the office.

She won't be testifying.

SENATOR THOMAS: Of course.

And will you be taking questions, or, no, you're just going to read the statement?

KATE POWERS: We won't be taking questions.

If you have questions, we would be happy to follow up with you after the hearing.

SENATOR THOMAS: Will do, that's great.

You may start, whenever.

KATE POWERS: So, good afternoon, Chairs Thomas and Savino.

My name is Kate Powers. I'm with the office of legislative affairs at the New York Attorney General's Office.

I will be reading the testimony of Clark Russell, who could not be here today.

Clark is the deputy bureau chief of the bureau on internet and technology, and he oversees the data-breach notification program, and all investigations conducted by the attorney general's office into data breaches affecting New Yorkers.

"More than ever, our way of life relies on electronic data.

"Indeed, almost every business transaction and communication involves electronic data.

"This information has value to wrongdoers, and has led to an explosion in the number of data breaches.

"We are losing the war.

"So, in light of that, we would like to thank you for the opportunity today to provide testimony in support of the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act)?

"In 2006, the attorney general's office received 300 data-breach notifications.

"In 2018, the office received over 1400 data-breach notifications.

"In the interim, we experienced data breaches involving tens of millions of records at companies like Home Depot, TJX, Uber, and Anthem, and hundreds of millions of records at companies like Yahoo!, Equifax, Marriott, eBay, and Target.

"The main cause of this explosion of data breaches is hacking, followed by employee negligence.

"Under current law, companies can compile troves of sensitive data about individual New Yorkers, but there is no black letter law requiring reasonable data security to protect this information unless the company is in a specific industry.

"Under current law, a company does not need to notify you if your online credentials or your biometric data gets disclosed to an identity thief.

"The Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act) seeks to update the law, consistent with what many other states have already done.

"First, the SHIELD Act expands the types of data that trigger reporting requirements to include user name and password combinations, biometric data, and HIPPA-covered data.

"If the company already had to provide notice to consumers pursuant to another federal or state regulatory scheme, they do not need to provide a second notice under our bill.

"It also implies" -- "applies when unauthorized third parties have access to the information, in addition to the current trigger for acquisition.

"This is important, because our experience investigating these types of breaches has shown us that, oftentimes, log files or other relevant electronic evidence necessary to prove acquisition of the private information is unavailable despite the fact that a breach occurred.

"The SHIELD Act also requires companies to adopt reasonable administrative, technical, and physical safeguards to protect private information.

"The standards would apply to any business that holds sensitive data of New Yorkers whether they do business in New York or not.

"The reasonable standard of care is in most all data security laws at the state and federal level, and provides a standard that is flexible. It can be adapted to changes in technology, sensitivity of the data retained, and the size and complexity of the business.

"The bill's flexibility is also evidenced by its carve-out of compliant regulated entities, defined as "those already regulated by existing or future data-breach regulations of any federal or New York State government entity, including the State Department of Financial Services' regulations, regulations under Gramm-Leach-Bliley, and HIPPA regulations," by deeming them compliant with the law's reasonable security requirement if the entity is compliant with their industry's regulations.

"Unfortunately, when a breach occurs, consumers often have limited options.

"Credit monitoring helps consumers identify suspicious transactions, but it only alerts the consumer after someone has already stolen her identity.

"Credit freezes stop wrongdoers from opening a line of credit in a consumer's name, but a thief can still file for government benefits in the consumer's name or file a fraudulent tax return.

"Of course consumers need to stay vigilant.

"They should create strong passwords for online accounts and use different passwords for differing accounts.

"In addition, to avoid computer viruses and online scams, they should avoid opening suspicious e-mail or clicking on suspicious hyperlinks.

"But the fact is, the best way to address the issue is to stop breaches before they happen.

"Businesses should only collect the information they need to conduct their business, and securely delete and destroy it when it is no longer needed.

"They should design and implement an information security plan, they should designate a person responsible for the plan, and educate and train their employees.

"Finally, they should continually review their plan and revise it as new threats emerge or their business changes.

"The Committee, and the Legislature in

general, has an important opportunity to address what is a defining issue of our time.

"By updating New York's data security, we can provide the protection that consumers need and deserve.

"We propose the SHIELD Act because we believe it is essential to help to addressing the threats posed by hackers and data breaches.

"We thank both of the Chairs for convening this important hearing, and we urge the Senate to pass the SHIELD Act before the end of this legislative session.

"Thank you."

SENATOR THOMAS: Thank you.

All right, can we have Panel 5, and the last one.

We're just going to wait for Marta to return before we start. All right?

(A recess commences.)

(The public hearing resumes.)

SENATOR THOMAS: All right, let's get started on our last panel here, Panel 5.

Again, forgive me if I slaughter anyone's name.

From DLA Piper, LLC, we have Andrew Kingman;

From the Business Council of New York State, we have John Evers;

From Ropes & Gray, we have Marta Belcher;

And from Soramitsu Company, we have James Loperfido.

All right.

So again, the rules:

20 minutes for the entire panel; so 5 minutes each.

Summarize your testimony. You don't have to read through it. We have it right here.

Our attention span is pretty off right now.

[Laughter.]

SENATOR THOMAS: So just keep it short, all right, guys?

Let's go.

JAMES LOPERFIDO: Is this thing on?

SENATOR THOMAS: Yes.

JAMES LOPERFIDO: Good, all right.

At the risk of sounding original after all the other testimony, and having less time than we originally thought, I'll try and abbreviate the best that I can.

Thanks for the opportunity to come.

Happy to share testimony relating to the

bills proposed.

My names is James Loperfido, a proud native resident of New York City, and I serve as the vice president of business development for Soramitsu, which is a global Japanese technology consulting company, with a global footprint that specializes in real-world applications of blockchain technology.

We're a member of the Hyperledger Group, a consortium of open-sourced blockchain solutions, endorsed by the Linux Foundation, which means we have nothing to hide.

My more valuable feedback will likely pertain to Bill 5642, the New York Privacy Act, as a generalist in the technology startup space.

So I'll speak to that now.

According to Domo's "Data Never Sleeps" report, we create 2.5 quintillion bytes of data every day.

With estimated growth figures, we'll produce about one high-quality picture's worth, or, 1.7 megabytes of data per second, per person on this planet, by the year 2020.

So the enormity of this problem is only growing in scale.

The importance of authenticity and providence of data, especially as it relates to an individual's digital identity, must be deliberately understood, managed, and protected.

The confluence of powerful technologies, including 5G, satellite Internet networks, artificial intelligence, the Internet of things, cryptocurrencies, and other technological innovations, will create a further explosion of data, both authentic and purposely deceptive.

Data pertaining to our individual likeness has specific value, and today that information is exchanged in a relatively opaque fashion for significant amounts of money.

That value persists after data change hand the first time, and we as individuals must be perennial stewards of our own to ensure its integrity and utility.

Ensuring we have unlimited knowledge with respect to how our data is shared, which our bill seeks to address; who it is shared with, and why, is crucial.

Much like the idea that 800 million to 2 trillion dollars a year is laundered each year around the world, we cannot possibly begin to

estimate with any degree of confidence how much of our personal data is misappropriated and potentially used against us.

According to Javelin Strategy and Research, there was 16.7 million victims of identity theft in 2017, resulting in $16.8 billion of fraud.

The question of data ownership and maintenance becomes a focal point amidst burgeoning technologies which creates some premise -- or, promise to correct our course.

The burden of proof, though, is a grand one for those fiduciaries responsible for our consumer data.

Data are extremely portable by their nature, either physically through hardware or virtually through shared access to a common database.

Both possibilities generally preclude auditability with a high degree of certainty, regarding that the data in question and its parent -- and their apparent security.

Accordingly, permanently relinquishing access to valuable personal data from the ether of the Internet becomes a very tricky task to both execute, monitor, or enforce.

Because of social-media platforms like

Facebook, credit services like Equifax, and index engines like Google, our digital identity and associated data points relegated to each of us remain visible to many.

The centralization of stewardship creates a power dynamic we have yet to comprehend the potential of.

The potentiality of decentralization, however, creates an entirely new paradigm to which we must pay attention.

How does a custodian or controller, according to the definitions in these bills, of personal data prove to the rest of the world that the data itself is secure and shared only with those who have been granted permission to access it?

How can we be sure that de-identified data are as such as, and remain so?

Can we guarantee that this de-identified data will remain decoupled from personally identifiable information if needed to be?

In an increasingly connected world, security, authenticity, and use of personal data are matters of both personal and national security.

To protect New Yorkers' and Americans' data, we must acknowledge that the nature of this value

exchange is global.

We must work hard to prevent the individual in a global, social, and economic framework from becoming just another statistic.

The Senate bills in question are a great start to shaping the standards required for transparent custody and transmission of personal data, but just begin to scratch the surface on the path to harnessing and fostering technological growth.

I implore the Committee members to -- responsible here to question the essence of data ownership, digital identity, and the impact their evolution has on the real world, especially with respect to a globalized economy.

Frontier technologies pose threats, but also creative and powerful solutions to concerns of data privacy.

Proactively creating a functional, ethical, and legal framework through careful promotion of their positive attributes, before rampant proliferation, is prudent.

I'm happy to speak to my understanding of blockchain technology, its relevance to digital identity, and the problems it has the potential to

solve to the best of my ability, and look forward to your questions.

Thank you.

SENATOR THOMAS: Marta.

MARTA BELCHER: Thank you very much for having me, to testify about the potential impact of these privacy bills on the blockchain industry.

So building on what James has said, I think there are two things that the New York State Legislature should take into account, with regards to blockchain technology, in forming this privacy legislation.

The first thing is that, blockchain actually has -- is very much in line with the ideals of this privacy legislation.

And building what on James said, there are a lot of potential applications for blockchain technology that actually can help with users, allowing them to control and own their data in a way they never have been able to before, and I'll give you some examples of that.

But, because of that, it's important that this legislation does not render blockchain technology to be automatically non-compliant, which is the concern here.

And -- so to give you some examples, I explained in my written testimony, and won't repeat here, sort of a -- a sort of basic Blockchain 101.

But I want to give you an example of how you can imagine blockchain technology helping users own their data.

So one of the things I talk about in my written testimony is the ability of smart contracts; being able to program your money.

So you could program your money to say, for example, for every second of a song that's playing, automatically transfer 1 one-millionth of a cent to the songwriter.

And one thing you can do with regards to data, is actually store data on a blockchain, along with permissions on who can use that data, for what.

So, for example, I could say:

Here's my health data.

Please store this on a blockchain with permissions that say, genomics -- you can use this for a genomics researcher.

A genomics researcher can use this, but the, you know, advertising industry can't.

Right?

And that could be -- that data could be tracked as it goes from party to party with those permissions continuing on.

And you could even program it to say, every time that any party uses this data for one of the things I've said they can use it for, they actually are going to automatically transfer me 1 one-millionth of a cent, right, without ever having to have an intermediary involved.

That's something I talk about.

And the ideals, of course, of blockchain and cryptocurrency are really in line with the ideals of privacy.

So as a result, I want to talk a little bit about the potential issues with these bills.

So the things that actually make blockchains so powerful and important are its decentralization and its immutability, but that actually creates some tension with this privacy legislation.

This was actually observed, sort of extensively, with the GDPR, which, of course, this legislation was actually, you know, based in part on.

And the first issue is that it really assumes a centralized data-governance model, whereas, as

I explain in my testimony, blockchain is actually decentralized.

So if you're looking, for example, to figure out who a processer or controller is, right, how does that work in a decentralized model where there isn't necessarily one person making the decisions; but, rather, it's spread out among all of the users?

Who then has that processor liability?

And how do you -- how do you, you know, take on that liability as just a regular user?

And then the biggest issue is really with the fact that the whole point of a blockchain, is that you have recorded the -- you have recorded the information permanently, forever. It cannot be deleted.

And, of course, one of the things in these bills is a requirement that you actually delete data.

And so that sort of fundamentally renders blockchain, potentially, non-compliant, without taking really special care to make sure that the language in the bills does not impose undue requirements on the blockchain industry that they simply can't comply with.

So, in short, and in summary, I think

blockchain is really, not a magic wand, but has a lot of, potentially, exciting applications, including applications in furthering the goals of this privacy legislation.

And as a result, I think it's very important to make sure that this legislation doesn't have the unintended consequence of stifling blockchain innovation in New York.

JOHN T. EVERS, Ph.D.: Chairman Thomas, Chairwoman Savino, I want to thank you for this opportunity.

My name is John Evers. I'm director of government affairs for the Business Counsel of New York State, the largest employer association in the state.

My comments are largely on the SHIELD Act, so let me say at the outset that we think it's not a perfect bill, but as in all things that are rapidly changing and advancing, it's a good start.

In fact, this bill has been the subject of well over two years of discussions, conferences, and negotiations between the business council and the office of the attorney general, and we're very pleased that, recently, Assemblyman DenDekker and Senator Thomas accepted amendments for this bill.

This legislation provides workable baseline standards for both security features and notification practices for New York State businesses.

Importantly, it recognizes existing standards that are universal for businesses nationwide, with clear reporting mechanisms that are largely already in place and best suited to protect the consumer.

Federal guidelines, as well as universal state standards, such as recent reporting regulations by DFS, are recognized and accommodated in this law.

This would avoid confusion that would be caused by having businesses and/or sectors being subject to multiple standards, an outcome that will only serve to complicate the system with no new discernible benefits to consumers.

This bill places into General Business Law and State Technology Law several provisions to stop hacks and improve electronic data security; its name.

First: The bill explains the interconnectivity of personal information and private information, and the use of this identifying information in conjunction with financial

biometrical information, except passwords, et cetera., to access and acquire personal data.

Second: The bill delineates the differences between internal, inadvertent breaches of private data, and external access and acquisition of the data.

In the case of the former, an inadvertent breach can be addressed as an incident of which data is accessed internally by those who should not be viewing the data, but no adverse impact has been caused, nor any evidence of malicious intent is found.

In these cases, the incident must be reported to the attorney general in writing, and the records maintained for five years.

One key provision in the bill is the adoption of new data security protections under a new Section 899-bb of the General Business Law, that places into state law the acceptance of existing federal and state security provisions.

These include, as the attorney general's staff just mentioned, Gramm-Leach-Bliley, HIPPA, and also Part 500 of Title 23 of the Official Compilation of Codes, Rules, and Regulations of New York State, and "any other data security and

rules and regulations" administered by official departments of the federal and New York State governments.

The attorney general review of the cases of breach, and determine what, if any, security practices and systems the entity had been following, and if proper notification procedures were followed.

As to "small-business entities," defined as those under 50 employees, or those under certain monetary thresholds, the new guidelines are placed into law.

Generally, these are defined, even in the bill, as reasonable.

Small businesses must maintain a, quote, data-security program that assures a baseline minimum data security standards, such as training of employees to handle data properly, software and updates that, quote, assess risk in both network and software design.

These protective provisions ensure data is accepted, processed, stored, and disposed of properly by small businesses.

We are pleased that, under this bill, any action by the attorney general must be brought within three years of the breach, or three years of

the attorney general being made aware of the breach, with the statute of limitations being six, except if evidence is found that the breach was hidden.

Initial drafts were far too expansive and provided no clear end point as compared to the triggering event.

The business council is also pleased that the new version of the bill maintain language, stating, there's no private right of action under this law.

We are grateful that this bill, and make it known, this is at least the fourth permutation of this legislation over two years, addresses various parts that we believe would provide work -- that would prove unworkable.

As stated above, the bill still contains some provisions that we do not support, such as a doubling, from 10, to 20 dollars, a civil penalty.

But it's gratifying that the new law holds government entities to the same standard as those in the private sector, and maintains the exact same baseline data-protection standards for New York State government and agencies, as well as similar reporting mechanisms.

And, further, it enlists the help of the office of information technology services to study

any breaches, and make recommendations for restoration and improvements to the system.

It charges ITS with delivering a report within 90 days on any breach, and mandates ITS develop, quote, regular training to all state entities relating to best practices for the prevention of breach of security of the system.

Overall, the business council supports the SHIELD Act.

Thank you.

SENATOR THOMAS: Thank you.

Andrew.

ANDREW KINGMAN: Good afternoon.

My name is Andrew Kingman.

I am here wearing two hats.

The first is as a compliance attorney in DLA Piper's cybersecurity and global privacy practice group.

I think my firm would ask me to point out that we are an LLP, and not an LLC.

[Laughter.]

ANDREW KINGMAN: The second is as counsel to the State Privacy and Security Coalition. We're a coalition of 25 retail, media, technology, communications, payment card, and online security

companies, as well as six trade associations. And we work on state privacy and cybersecurity legislation nationwide.

I also, just to follow up on some of the questions from the prior panels, may be able to help clarify some of the questions around the New York Department of Financial Services' cybersecurity regulations, as well as some of the questions around online political ads and the online ad ecosystem.

So we can discuss that perhaps in the question time.

I would like to first discuss The SHIELD Act.

To echo many of my colleagues, it's something that we also have been working with the attorney general for the last couple of years on.

We believe that, overall, it provides sensible updates to New York State's breach law.

We work on breach laws nationally.

And, so, have offered amendments that would seek to conform this statute to some of the best practices found nationwide.

In a data-breach scenario, this is beneficial to the consumer. It increases the efficiency with which consumer notifications can be put together.

The greater the uniformity across state lines

in requirement, the less time it takes to draft notifications that comply with those requirements.

I'd just like to outline, briefly, a couple of the changes that we would like to see.

And again, overall, we are supportive of the direction of this bill, and appreciate the Legislature's effort this year. I know it's been the product of several sessions of work.

The first would be, to tighten up the "biometrics" definition, and eliminate the clause dealing with "a physical or digital representation."

It's not necessarily clear what that would be.

It also could implicate things like irreversible hashes of biometric information, which don't pose a security threat to consumers.

To answer your question earlier, Senator Thomas, about what the appropriate threshold is for when consumers should receive notification of a data breach, we believe it's, as many states have gone down this path as well, the inclusion of what's called a "harm trigger."

So, making sure that consumers are notified when there's a reasonable likelihood -- or, excuse me, a likelihood of harm or identity theft or fraud

to that consumer, that that's an appropriate threshold with which to notify consumers, particularly with an access standard, when it's not always clear what information has been acquired; whether a hacker has actually taken that information or not.

Allowing an assessment of whether a consumer is subject to some degree of possible harm is an important consideration, and sort of the next step in determining what that type of situation is.

So, we detail our rationale for the amendments, but those are two of the main amendments that we would like to further see.

But again, supportive, generally, of the direction of this, and appreciate the effort.

Many of my colleagues already today have expressed, you know, some of the common concerns around the New York Privacy Act.

I'd just like to add a couple of pieces of information there.

The first, you know, I think there's been a lot of doubt expressed about the "data fiduciary" standard, for a number of reasons.

I think, from a compliance standpoint, it's important, when we're passing very complicated laws

that will impact, really, every sector of the New York economy, it's important that businesses be able to build a compliance program around those types of laws.

When laws are subject to subjective standards, like some of the issue -- like some of the elements of the privacy harm or privacy risks that are found in the "data fiduciary" standard here, it's impossible to build a compliance program where a business can assess how to deal with the processing of that data.

And, so, I think establishing objective standards for -- in requirements is a core component of any privacy legislation.

I am not -- you know, our group works on privacy legislation nationally.

In over half the states this year, we have seen bills that have attempted to, you know, provide consumer rights or increase privacy protections.

We refer to them as "omnibus privacy bills."

This is the first bill that has attempted to introduce a "data fiduciary" concept, and so it's not something that has been really considered before, and it's largely academic right now.

And I think it's a little bit premature to

insert that, particularly coupled with the private right of action, which I'll discuss in a minute here.

But, you know, when we're looking at privacy-- okay.

SENATOR THOMAS: If you want to quickly summarize.

ANDREW KINGMAN: Well, I was just going to say, when we look at privacy legislation, we operate from a framework of three things:

One is, ensuring that legislation does increase consumer control and transparency.

But with that increased transparency also comes increased cybersecurity threats, because, if a company is making more information public, there are increased vulnerabilities to that.

So we want to balance some -- we want to make sure that businesses retain the tools to defend their consumers' information, their employees' information, their company information, from, you know, persistent threats.

And then the third piece is operational workability, as I said, making sure that businesses can actually comply with the law in a reasonable way.

SENATOR THOMAS: All right, excellent.

I'm going to hand this over to Senator Savino.

SENATOR SAVINO: Thank you.

So I want to focus a bit on the blockchain issue, because, as you know, earlier this year, we passed a blockchain bill in the Senate.

I don't think the Assembly has done it yet, but adopting a smart contracts, blockchain, statute.

So I'm a little, obviously, interested in how you believe the Senator's proposal will disrupt the blockchain.

So if you could explain it a little bit more to me, because my understanding of blockchain, and, believe me, I'm no expert on this, I'm learning as I go, is it --

JAMES LOPERFIDO: Nobody is.

SENATOR SAVINO: Right, exactly.

-- it's not really for the -- to collect data. It's to -- it's transferring it.

But nobody really owns the data.

It's like it's in little, small pieces, right, it's like a ledger, it's like a digital ledger, so to speak, right, of secure transactions.

So in what way would his bill disrupt

blockchain?

And how could we fix it if we were to amend the language?

MARTA BELCHER: Sure, absolutely.

So you can actually store, sort of, any length of data on a blockchain.

And one thing that the bill talks about, of course, is the definition of, you know, "private information" and "personal data," and what is actually included there.

And one thing, that it's really important to clarify, that I think is sort of a gray area right now, is, when data is actually encrypted and stored in an encrypted form, whether that is going to be something that still counts as "personal information" covered by the bill.

So one thing that you can do is, basically, create what's called "a hash," which is, basically, a digital fingerprint of data.

And I think it's -- that's very important for blockchain technologies, and it's very important to make that clear, that that -- that "a hash" would not count as "personal data" under these bills.

SENATOR SAVINO: I see, so there is a potential solutions to this.

SENATOR THOMAS: Uh-huh.

SENATOR SAVINO: He's whispering behind me (looking over shoulder).

JAMES LOPERFIDO: I think there's some misunderstanding, excuse me, with respect to the nature of public blockchain versus the private blockchain, and also the distributed ledger technology, which may or may not include a blockchain necessarily, but, a set of series of distributed ledgers, maintaining a copy of the same information.

And adding on to what Marta was saying about, you know, how things are encrypted, and where they're stored, and the idea that some encrypted information can be stored on a server without that server having access to that information.

Right?

These are very, you know, nitty-gritty concepts, but very important in how data is owned, transferred, and viewed.

Right?

So within a private permission blockchain, for example, you could store data, and assign both write and read permissions to entities involved in the maintenance and transfer of that data.

So -- and, you know, you could very easily preclude public entities, or, whomever, really, from accessing that data.

And with respect to a blockchain, yes, it's generally immutable, but there are other versions of distributed-ledger technology, where private-permission scenarios can allow for the actual mutability of data when it's crucial.

So there are many -- it's much more of a spectrum than a black-and-white type of thing, is kind of what I'm getting at.

SENATOR SAVINO: Thank you.

SENATOR THOMAS: So, again, with the blockchain companies, right, this legislation is trying to rein in companies that share and sell information, that uses personal data to target consumers.

Are blockchain companies in the business of doing that?

JAMES LOPERFIDO: So when I think of private information, I kind of default to Facebook owning most of it, in many ways.

And, you know, there's certainly, you know, what I'm seeing in, you know, consumer-facing businesses in the blockchain space, is the potential

to disrupt the idea that your data is given away, and that it's then later monetized.

You know, and you guys are addressing these ideas.

But what I'm seeing is that, there's an incentive, an increasing awareness, that you can own your data and distribute it as you'd like.

So, you know, there's definitely the good, bad, and the ugly in the industry, especially with respect to public cryptocurrencies.

But, in terms of owning data, and distributing it as needed, on a permission basis, there's a lot of value in that, I think.

I don't know if that well answers your question, Senator Thomas, but...

SENATOR THOMAS: We're joined by Senator Bailey.

To Andrew Kingman, you talked about the data fiduciary, and how it's difficult to comply with the duty of loyalty to the consumer and the duty of loyalty to the board members.

Why can't you do both?

I mean, I had a panelist that came in earlier, that talked about companies already doing this.

You know, when products are created, there's products liability. You know, you're trying to make sure the product doesn't harm the consumer; but at the same time, they have a duty of loyalty to the shareholder.

Why can't we do both for data privacy here?

ANDREW KINGMAN: Sure.

I think -- I think, first of all, there are other ways to ensure that businesses are taking care, and appropriate safeguards, for their customer information.

The department of financial services' regulatory regime is one for the cybersecurity requirements.

The requirement in the SHIELD Act, that businesses institute reasonable safeguards, is another.

In Ohio they passed a bill, providing an affirmative defense for companies that follow well-recognized, like The National Institute of Standards and Technologys' cybersecurity framework, that, following that, and being in reasonable compliance with that, as new additions are released, provides an affirmative defense against enforcement action.

So there are lots of ways to incentivize, and to provide more oversight over the way that companies are safeguarding their information.

I think a "data fiduciary" standard, particularly one such as this, you know, reading it, and trying to advise a client on how to comply with it, would be very difficult.

So, if the question -- just as an example, right, so it would allow: A private right of action by consumers against a company, based on a standard of effects on an individual that are not contemplated by the individual, that are, nevertheless, reasonably foreseeable by the controller assessing the privacy risk that alters the individual's experiences.

So, you know, an extreme example of this would be, like a smart refrigerator that regulates power flow, that spoils the milk, that the consumer wasn't expecting that to happen.

Does -- does that -- is that grounds for a private right of action?

Right?

So, these are the types of reasons why it is difficult to implement something that is vague and subjective like that.

And I think to the point of the private right of action, which we strongly oppose, you know, Senator Savino, earlier you said that, you know, lawyers only get paid if they win.

You know, they also get paid if they settle.

Right?

And so -- just, you know, I've provided some links in my testimony --

SENATOR SAVINO: I think the point I was trying to make is, they don't file cases if they don't have a reasonable expectation they're going to get a settlement out of or win.

ANDREW KINGMAN: Well, I cite a couple of studies, actually, in my testimony; one dealing with a study of over 150 class-actions filed federally, and, between 2010 and 2012.

And not a single case was resolved on the merits in favor of the plaintiffs.

And, you know, it's worth just absorbing that for a minute.

31 percent were dismissed by a Court on the merits, and only 33 percent of the cases settled.

But more than that, the studies show that what is effective in class-action lawsuits is that it's a transfer of capital from the company to the

trial lawyers.

Right?

So that -- the other statistic that I cite shows that the actual take-home for attorneys, compared to the -- because attorney's fees are based on the total possible number of class-action participants, rather than the people who actually sign up and get the money, that their fees are often 300 to 400 percent of the actual take-home of what the consumers are getting.

So, to claim that it's a benefit to consumers, or that it provides meaningful recourse for consumers, I don't think that the data actually bears that out.

SENATOR THOMAS: A couple of the earlier panelists also talked about First Amendment and commercial-speech rights.

What are your thoughts on that?

ANDREW KINGMAN: I have fewer thoughts on that. It's not quite in my wheelhouse, so I don't want to get too far over my skis there.

SENATOR THOMAS: Okay.

ANDREW KINGMAN: I'll let prior panelists' speak -- testimony speak for -- to those points.

SENATOR THOMAS: All right.

So, thank you all.

SENATOR SAVINO: Thank you.

SENATOR THOMAS: So I'm going to close out this hearing.

I want to thank Senator Savino for sticking by me for a couple of hours.

And also Senator Liu for being here to ask questions.

And I also want to thank our staff that worked so hard on putting this together, and the panelists that participated today.

Like I said at the start of this hearing, we can give New Yorkers their privacy rights and allow our economy to thrive.

I'm looking forward to working with all of you to make the lives of consumers better.

Thank you so much.

(Whereupon, at approximately 1:21 p.m., the joint committee public hearing concluded, and adjourned.)

---oOo---