Statement of

Justin Brookman
Director, Privacy and Technology Policy
Consumer Reports

Before the

New York State Senate
Standing Committee on Consumer Protection
and
Internet & Technology

On

Protecting Consumer Data and Privacy on Online Platforms

November 22, 2019

Thank you for the opportunity to speak today. My name is Justin Brookman, Director of Privacy and Technology Policy for Consumer Reports,[1] an independent, nonprofit member organization representing 6 million consumers nationwide. Consumer Reports appreciates the committee's commitment to exploring the need for privacy and security legislation. In the absence of action from the federal government, states are taking important steps toward establishing baseline privacy protections. It's important that any state privacy legislation has strong protections that advance consumer rights, ensures privacy by default, holds companies to real limits, and is backed up by strong enforcement. Last year, we supported the SHIELD bill which provided important new cybersecurity protections for New York residents,[2] and we are gratified to see the legislature seriously considering privacy legislation in this session.

Consumers want more, not fewer, legal protections over their personal information. For example, 92 percent of Americans think that their Internet Service Providers should provide greater control over the sale of their personal information.[3] More than half don't trust social media companies to keep their information safely protected.[4] And almost three-quarters said that it's very important to have control over their information.[5] Recent scandals involving the illicit sharing or sale of personal information without consent, such as the Facebook-Cambridge Analytica incident,[6] and reports of unauthorized sharing of location data, for example by the Weather Channel app, have revealed broad unease about data sharing.[7] Clearly, consumers value their devices, connected products, and other apps and services, but they don't have the confidence that their information is protected.

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

---

[1] Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] S. 5575 (2019).

[3] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, CONSUMER REPORTS (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data/.

[4] Lee Rainie, *Americans' Complicated Feelings about Social Media in an Era of Privacy Concerns,* PEW RESEARCH CTR., (Mar. 27, 2018) http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy- concerns/.

[5] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[6] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions,* N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump- campaign.html.

[7] Joseph Cox, *I Gave A Bounty Hunter 300 Dollars. Then He Located Our Phone*, MOTHERBOARD (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

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 FTC, is vastly underpowered and under resourced.[8] This is why state action is so important and should not be chipped away. Baseline protections—analogous to mandatory seat belts or airbags— are needed so consumers can safely use apps, social media, and online services without having to compromise their rights to privacy.

In advance of this hearing, we reached out to Consumer Reports members who live in New York to ask for their stories about times when their personal information has been misused: I'm attaching some of that feedback we received from these members at the end of my testimony.[9]

With regard to Senate bill 5642, there's a lot of like in this bill, and we applaud Senator Thomas for his leadership in proposing it. It certainly has a lot of elements that we're looking for in a comprehensive privacy bill:

- **Access** to the data that companies have about us, and the ability to **move** that data to another service, or **delete** it altogether — I think these should be basic rights that people expect from companies. We've seen these sorts of rights passed in Europe and California, it's great to see them included in this bill.

- Expanded **security** obligations for all personal data — the SHIELD Act was a great start in adding safeguards for certain data, this bill takes the next logical step in requiring companies to use reasonable safeguards to protect *all* user data from attack.

- We are pleased that the bill has **strong enforcement**, including enforcement not just by regulators but by individuals whose personal information may be misused or exposed: Regulators alone don't have the resources to police all the data collection and sharing going out out there — I worked in the Internet Bureau of the New York Attorney General's office but we only had a handful of attorneys. In California, where there's a new privacy law, the Attorney General Becerra has said he only has the capacity to bring a handful of cases a year[10] — ordinary

[8] Justin Brookman, *Facebook Fine Reveals Congress Has Set Up FTC to Fail*, THE HILL, https://thehill.com/opinion/cybersecurity/456049-facebook-fine-reveals-congress-has-set-up-ftc-to-fail.
[9] These stories were submitted by members. They have not been checked by Consumer Reports for accuracy. The stories reflect the views and opinions of the submitting members and may not necessarily reflect the views and opinions of Consumer Reports.
[10] Yuri Nagano,
California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court, SAN FRANCISCO PUBLIC PRESS (May 15, 2019),

citizens and public interest groups need some capacity to petition the courts to protect our rights as well.

That said, we do have concerns about the bill, there are certainly parts that are very similar to a bill in Washington state that privacy advocates aggressively opposed last year.[11] This bill is largely stronger than that bill, but there are areas that should be improved.

- Clarify the rules on **sharing** and **secondary use** — The most difficult part of any privacy law is how to regulate the secondary use and sharing of personal information. People generally understand that a lot of data collection is functionally necessary for products and services to work. Where they get concerned is when that data is repurposed or shared for unrelated reasons. When we go to the grocery store, we understand that the company is going to collect credit card data for processing, or might remember what we purchase if we're part of a loyalty program. But we don't expect that the grocery store will sell information about what I buy to a data broker for advertising or other reasons.

    - This bill is unclear as to what the rules are for secondary use and sharing. At times, it sounds like affirmative permission is required for sharing, at others it sounds like there need only be some ability to opt out.

    - On **sharing**, our preferred approach would be to broadly prohibit secondary sharing or selling of data with third-parties apart from what's functionally necessary for a product to work. I don't want to recreate the GDPR experience where tons of websites just bombard users with dubious permission requests to track users. I think companies shouldn't bombarding consumers asking for permission to sell data to third parties, they just shouldn't be doing it.

        - If ultimately, the legislature decides it wants to go with a less aggressive opt-out approach like we've seen in California, the bill needs to allow consumers to exercise *global* opt-outs, so they don't need to opt out of sale site-by-site, or store-by-store. So a consumer can turn on Do Not Track in their browser, or add their email address to a Do Not Sell database. Other opt-out bills do provide for global opt-outs — the California law requires this,

https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.

[11] Letter from Consumer Reports *et al.* to The Honorable Christine Rolfes, Chair, Members of the Senate Ways and Means Committee re SB 5376 (Protecting Consumer Data) - OPPOSE (Feb. 21, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf.

Senator Wyden has a thoughtful approach on how to do this. Again, we'd prefer to see data protected by default, but if you rely on opt-outs, they need to be powerful and universal.

- On **secondary use**, right now the bill has companies conduct risk assessments and make internal, opaque decisions as to what data uses are bad for the consumers. I think that gives too much discretion and leeway to companies to do as they see fit with my information. Instead, it makes more sense to simply enumerate what reasonable secondary purposes are: and these can be fairly broad, allowing first-party usage for analytics, or research, or even personalization and marketing. But I wouldn't leave it to companies to decide on their own what's "risky" and what's ok.
    - I think this is one of our disagreements with the idea of giving companies "**fiduciary**" responsibilities over data. We worry that this formulation gives too much power to companies to decide what's good and bad for consumers and their personal information. Instead, the law should provide clear and enforceable rules around what companies can do with our data.

- Another important concept that should be included in this bill is the principle of **non-discrimination** — that is, a company shouldn't to penalize or charge different prices to an individual who exercises privacy rights. Certainly, more and more industries are dominated by a few companies — and in those cases, they certainly have the ability to set unduly onerous terms for data collection. But more fundamentally, privacy shouldn't just be a luxury for the rich — all people should be entitled to a zone of personal privacy that they can be coerced into bartering away. Certain rights are considered to be "inalienable" — we can't sell our right to vote away to an employer or a big company. I think we need to think of privacy in the same vein, and carve out some spaces where we can just trust that our data isn't being collected and sold to the highest bidder.

- To accomplish the intended purpose of this law, a number of the bill's **definitions** need to be substantially tightened:
    - For example, the current definition of **de-identified** is ambiguous, and could potentially allow companies to keep data in a form that could be trivially reidentified. This is really important because the bill gives companies broad leeway to do whatever they want with deidentified data. We're ok with that but only if the data really is de-identified. So we

suggest that this language be revised to match the Federal Trade Commission's definition of de-identified to ensure that companies believe in good faith that deidentified data sets reasonably could not be reassociated with unique individuals, even if a company was motivated to do so.

- Next, the current definition of **sale** is extremely narrow, and would permit much, if not most data sharing that is the intended target of the bill. Already, you've seen advertising companies saying they're going to get around the CCPA by claiming that most online data transfers aren't "sales' — and this bill's definition is even narrower. We propose to expand this definition to cover the whole universe of secondary data sharing.

- The **personal data** is defined as "information relating to an identified or identifiable natural person" — that leaves open some ambiguity as to whether it applies to online data that might only be tied to a cookie, or IP address, or a device identifier. Consumers spend a lot of their time web browsing or in apps that don't necessarily know their name — but they still have an interest in stopping the deluge of targeted ads or having their behavior tracked from site to site. There's definitely increasing awareness that this type of data is personal and still shapes of our everyday experience[12] — it could potentially be tied back to us one day, but that's not the only reason we might want to limit its collection and sale. For that reason, we suggest modifying this definition to reflect the language in the CCPA and other bills defining personal information as data that "identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device."

- And finally, we do support an exception for **service providers** to allow companies to share information with other companies working solely on their behalf. There's definitely value to allow companies to outsource functionality to more experienced companies like cloud providers or database managers. But we'd like to see some more protections around those relationships — specifically we'd like to see requirements that service providers (1) can't reuse data for their own purposes and (2) can't merge and combine data from different controllers.

[12] Jessica Rich, *Keeping Up with the Online Advertising Industry*, FED. TRADE COMM'N (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

- The **exemptions** in Section 1107 should be narrowed somewhat — I think the use cases laid out are generally sensible, but there's no notion of reasonableness or proportionality required for purposes such as security and fraud prevention. Mark Zuckerburg has said for example that Facebook collects data about all the other websites and apps people use because it might help Facebook detect fraudulent accounts.[13] In that case, the extensive data collection doesn't seem reasonably necessary and proportionate for the incremental security benefit. The CCPA, for example, limits data processed for exemptions to what's reasonably necessary and proportionate for the exempted purposes, and we'd like to see that constraint introduced here as well.[14]

- And finally, we'd suggest eliminating — or at the very least narrowing — the **preemption** provision currently included in the bill. As currently written, it would broadly preempt *any* local laws having anything to do with the processing of personal information. This could inadvertently interfere with any number of local ordinances such as laws affecting schools and landlord/tenant issues. Even with regard to commercial data processing, this bill should allow cities to adapt to emerging threats and pass new protections not addressed or even contemplated by this law. For example, some New York cities have considered legislation regulating or limiting the use of facial recognition in public places;[15] cities should be allowed to enact additional protections if they deem that's in the best interest of their citizens.

So we obviously have some suggestions for improvement, but I do want to emphasize that we are extremely excited about this bill and look forward to working on it. Thank you again for introducing it, for holding this hearing, and for inviting Consumer Reports to testify. I'm happy to answer any questions you might have, now or as you continue to work on this bill.

[13] Mark Zuckerberg, *The Facts About Facebook*, WSJ (Jan. 24, 2019), https://www.wsj.com/articles/the-facts-about-facebook-11548374613.
[14] Cal. Civ. Code § 1798.140(d).
[15] Dean DeChairo, *New York City Eyes Regulation of Facial Recognition Technology,* Roll Call (Oct. 29, 2019), https://www.rollcall.com/news/congress/new-york-city-eyes-regulation-of-facial-recognition-technology.

Appendix: Consumer-Submitted Digital Privacy Stories

Any website which incorporates AI in their technology solution is an invasion of privacy an breach of consumer personal information data. One of the many examples include when I purchased a product at Amazon, only to find the product on a completely different website I visited. Amazon did request my authorization or consent to share my shopping product with any other company or affiliate company on the web. Additionally, my personal information data and credit card details was not deleted from Amazon and affiliate companies database when I deleted the information. This is misinforming the consumer when the consumer assumes (which I never assume) the personal information data and credit card details is deleted/removed/expunged from Amazon and affiliate company databases. Beware of AI!
--C., New York, NY

I got sick of being targeted by online ads on every website, based on my browsing history and purchases I'd made. So I installed a paid VPN (Virtual Private Network), Sophos At Home realtime anti-virus, anti-malware, anti-ransomware protection. If I really want safety, I'll use the Tor Browser on top of that, but Opera is good for most things. Now The New York Times, for which I pay, is asking me to allow ads, ha!

But I also pay for Amazon Prime, but if they can't track me, I can't stream or download from them. I'm not getting all the benefits of Prime membership; maybe a class-action suit is in order? After all, I pay for the service and I'm not getting what I pay for.

Google? Twice a year I clear unnecessary emails by marking them as spam and unsubscribe; it's a chore. To think government can protect us from this seems absurd to me.
--Cameron, Kingston, NY

I do notice marketing on my Facebook linked to my web browsing interests and online purchases and I have concerns as to whether my private information is protected. Would feel more secure with legislation to enforce my privacy.
--Christine, Camden, NY

I have a condition that emergency service providers might need to be aware of if I suffer a health emergency. Shortly after putting that information on the wallpaper of my cellphone to facilitate making EMTs aware, and using an app designed for that specific purpose, I began receiving ads for medical services using the precise language I had used in describing that condition.
--Dennis, Albany, NY

I receive more than 200 emails daily, it's out of control - it takes me too much time to "unsubscribe" from them & then they keep on coming anyway. It's obvious that Amazon keeps records of everything you've ordered & they advertise the same/similar items; as does FBk. The robocalls are repetitive as well; even if you hang up on them without any interaction, they continually call again. I'm registered with the DMA for no soliciting & even have "nomorobo" for calls, but they still get through. As a user, I should absolutely have the right to deny any internet company from selling my personal information for their profit.
--Holly, Brewster, NY

Of course I like everyone else received unsolicited e-mails and phone calls based on information searched or browsed on the internet and social media. It's annoying and at times have actually interrupted legitimate transaction or conversations. But please also help citizens protect their smartphone accounts from ruthless illegal hacks.
--James, Pearl River, NY

- Unsubscribe requests ignored or significantly delayed implementation. From political campaigns as well commercial interests.
- Advertising pops up on certain websites after any product search on Google.
- I left Facebook 1.5 years ago for privacy and security reasons. I believed I was targeted by political ads.
--John, Bellmore, NY

Between the obvious use of browsing history to inundate me with ads for products and services. The robo calls have taken over my day. No less than 10 a day and sometime many more are disrupting my life. Please help shut this down!
--Kent, Southampton, NY

I am flooded with emails from advertisers that I did not signed in for, but only visited.
--L.A., New York, NY

I looked up an address of a Hotel in New York City. I was interested only in address, not rates nor availability. I was meeting a friend who was going to stay at that hotel. Several days later, I received email and pop up ads for that same Hotel...Coincidence!!!I think not. There have been many other advertisements on my computer prompted by my earlier searches.
--Lisa, Gansevoort, NY

When I go online and look at something for sale, ads for that product pop up on other websites, making me feel I'm being watched as I browse products. It's like having someone follow you in the aisles of a store, then waving things you've looked at in your face.
--Marie, Baldwin, NY

I often receive ads in my email, both legitimate and clearly phishing expeditions, which I did not sign on for and have no idea how the sender got my email address. I opt out of information sharing whenever possible and almost never click on "more info" or "agree to receive email on products or services" buttons. But still they come. Sometimes I unsubscribe. For more suspicious messages, I am wary of unsubscribing, and simply mark them as spam. After unsubscribing they would pop up a few days later. Thanks for doing this work!
--Mark, Jamaica, NY

Increasingly, I'm seeing online ads that are apparently based on information that comes from phone conversation information. Other ads come from a particular article I read online. I'm feeling quite concerned about the massive invasiveness of all data collection in my life. I don't believe this is simply a case of paranoia, but an unchecked corporate manipulation far worse than the purported crimes of Cambridge Analytica.
--Matthew, Palmyra, NY

Why are social security numbers, birthdays, phone numbers, even street addresses, and other information collected by websites when not specifically needed? And then, when mishandled, or if there is a data breach, it's all out there!
--Neil, Forest Hills, NY

I shop at Staples etc. regularly. I receive their sales offers by emails. But most annoying thing is that their ads pop up 'forcefully' on my PC screen at bottom right corner, or, in between a 'you tube' program I am watching. I had to fix the problem by going through my Google Chrome help desk.
--Pradeep, Flushing, NY

I had two businesses refuse me as a customer because I wouldn't give them my personal information.

One occasion was when I borrowed someone's truck on the understanding that I have the oil changed before returning it. I went to [redacted] in Amherst, NY and the manager asked me for my phone number, address, and e-mail address. I asked why he needed that information to do an oil change. He said he needed it for the invoice. I told him I didn't want to divulge my personal information and that he didn't need it just to change the oil in the truck that I had borrowed. He responded by saying if I didn't provide the information he asked for, he couldn't/wouldn't do the oil change. I left without having any service performed on the truck.

Another occasion was when I went to a hearing specialist [redacted] in Tonawanda, NY to get a set of custom in-ear monitors made . . . The hearing center wanted my address, phone number, e-

mail address, my health insurance card, the name of my physician, etc. I asked what for. I just wanted to get some custom in-ear monitors made and that I was going to pay for them outright. They said they needed to onboard me as a patient. I replied that I had no interest in becoming a patient. I just wanted some ear molds so I could have some custom fitted in-ear monitors made. Like my experience with [redacted], we hit an impasse. Unless I surrendered my personal information, they likewise refused to do business with me.
--Robert, North Tonawanda, NY

I constantly get pop ups from advertisers. There is no privacy. My wife who is a therapist and frequently works with young children and teenagers receives pop up ads based on her purchasing history. These pop ups sometimes contain advertisements for undergarments and other personal items. Very embarrassing. Mr. Orwell was indeed a prophet.
--Steven, Hicksville, NY

I have been a DirectV customer for many years. AT&T bought them, and when I tried to access my DirectV account online, I found that I needed to sign up for AT&T access. On reading their terms of service agreement, I found two sections which seemed to say that my personal information would become their property forever and they could do whatever they want with it. I wrote them (and you) and said I would never agree to those clauses and asked for another way to access my account online. I was then traveling and received an email sometime later saying that [redacted] had tried to call me and wanted to talk about my letter. As soon as I returned home, I called the number he sent me at least three or four times. After the last call, he sent me another email with a lame excuse that they had switched their phone system. Imagine, communication is their business!! He said my privacy would be protected. At the bottom of his email was this statement: "Any other use, retention, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited." This is the old, What's yours is mine and what's mine is mine. I would change my television service, except my husband has a meltdown when I mention it!
--Suzanne, NY

I purposely do not download APPS because if you read the fine print on almost every APP, they tell you in writing that by downloading their APP you are consenting to allow that company who's APP you downloaded , to sell or distribute your private information, which you never gave them to begin with.

How is ANY OF THIS LEGAL.

Legislation MUST be passed that completely does not allow ANY company to simple inform you that by purchasing or downloading their product that they are allowed all your information.

If you by a product, a company does cannot be allowed your information. That is by definition, extortion. Plus abs simple. How I know my information has been sold to thousands of companys? Because I have opted out of all APPS and do not give my information out to anyone for over two years. I'm getting bombarded and invaded daily today and this is a violation and I feel violated , stolen from and abysses by this.

Pass new laws NOW to stop this violation and theft.
--Tiger, New York, NY