Statement of

Justin Brookman
Director, Consumer Privacy and Technology Policy
Consumer Reports

Before the

Council of the District of Columbia
Committee of the Whole

on

Bill 23-215, Security Breach Protection Amendment Act of 2019

November 12, 2019

John A. Wilson Building
Room 412
1350 Pennsylvania Avenue, NW
Washington, DC 20004
11:00 am

Consumer Reports[1] appreciates the opportunity to provide testimony on the need for strong data security and data breach notification requirements. Residents of the District of Columbia deserve additional protections, because consumers remain more vulnerable to data breaches than ever. Companies have dramatically expanded their data collection practices as they have found new ways to monetize consumer data, but incentives to protect consumer data from unauthorized disclosure remain inadequate. For example, The Equifax data breach of 2017 led to the disclosure of the personal information, including Social Security numbers, of over 145 million Americans—about half of the United States population—leaving them susceptible to identity thieves seeking to open credit in their names for years to come.[2] The breadth and depth of personal information involved could all-too readily also be used to defraud and otherwise manipulate the individuals affected.[3]

To that end, Consumer Reports supports Bill 23-215, the Security Breach Protection Amendment of 2019, a bill that would patch significant weaknesses in the District of Columbia's existing data breach laws. The bill expands protections over personal data by requiring businesses to implement reasonable safeguards over personal information to help prevent data breaches. It also extends existing data breach notification requirements to cover additional categories of sensitive data, including information that can be used to access an email account, passport numbers, taxpayer identification information, biometric information, DNA profiles, and

---

[1] Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications. It employs its rigorous research and testing, consumer insights, journalism, and policy expertise to inform purchase decisions, improve the products and services that businesses deliver, and drive effective legislative and regulatory solutions and fair competitive practices. Consumer Reports works for pro-consumer policies in the areas of telecommunications and technology, financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace.

[2] Jeremy C. Owens, *The Equifax Data Breach, In One Chart*, MARKETWATCH (Sept. 10, 2018), https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07.

[3] Kelli B. Grant, *Your Next Worry After the Equifax Data Breach: Fake Tax Returns*, CNBC (Oct. 9, 2017), https://www.cnbc.com/2017/09/18/your-next-worry-after-the-equifax-breach-fake-tax-returns.html.

medical information, so that companies are required to notify consumers if the data is breached. We urge members of the DC City Council to support this common-sense legislation to better protect consumers' privacy and financial security.

While breaches can occur even when companies take reasonable precautions, many breaches have been caused by companies' carelessness and lack of accountability. It's time for the District of Columbia to make data security a priority, and to pass a law establishing these essential consumer protections. Without a clear regulatory framework for data security, companies have insufficient incentives to be better stewards of consumers' personal data. The market simply will not fix this problem—indeed, it was not until the states began enacting data breach laws in the early 2000s that companies even disclosed their breaches to the public. Although all of the states and the District of Columbia have now passed data breach notification laws,[4] only about half of the states have data security laws—nor is there an across-the-board federal requirement—which is needed to prevent breaches from happening in the first place.[5] This bill fills an important gap in protections, and by passing this bill, the District of Columbia will help encourage the remaining states to follow suit.

The damage caused by data breaches is wide-ranging. Security breaches of retailers, financial institutions, data brokers, businesses, government agencies, and universities are now commonplace. There were over 2,000 data breaches in the United States and abroad in 2018.[6] One survey revealed that nearly one-third of United States consumers were notified of an

---

[4] *See 2019 Security Breach Legislation*, NAT'L COUNCIL OF STATE LEGISLATURES (July 26, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx.

[5] *See Data Security Laws, Private Sector*, NAT'L COUNCIL OF STATE LEGISLATURES (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[6] *2019 Data Breach Investigations Report, Executive Summary*, VERIZON 2 (2019), https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf [hereinafter Verizon Data Breach Report].

unauthorized disclosure of their information in 2017.[7] In what is widely considered the largest hack of personal information in history, web service provider Yahoo's 2013 data breach exposed the information of anywhere from one to three billion consumers.[8] A data breach in 2015 of the U.S. government's Office of Personnel Management's background investigation databases exposed the sensitive data of 21.5 million individuals.[9] And these breaches have a significant impact on consumers. Americans lost nearly $3.4 billion to new account fraud in 2018, up from about $3 billion the previous year.[10]

Data breaches are harmful for businesses—in 2018, the average cost of a breach to companies globally climbed to $3.9 million, a 12 percent increase over the past five years.[11] Summit Credit Union of Madison, Wisconsin testified that fraudulent charges related to data breaches cost them hundreds of thousands of dollars in 2017, not even counting the costs to replace credit and debit cards and for staff time to help resolve issues.[12] And as Pew Research Center points out, these data breaches are causing consumers to lose their faith in institutions, as Americans "lack confidence in various institutions to keep their personal data safe from misuse."[13] Most of these breaches—43%—targeted small businesses.[14]

---

[7] Press release, *One-Third of Consumers Notified Their Data Was Breached*, HSB (Mar. 22, 2018), https://www.businesswire.com/news/home/20180322005652/en/One-Third-Consumers-Notified-Data-Breached.

[8] Dell Cameron, *The Great Data Breach Disasters of 2017*, GIZMODO (Dec. 27, 2017), https://gizmodo.com/the-great-data-breach-disasters-of-2017-1821582178.

[9] *Cybersecurity Incidents*, OPM.GOV, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[10] *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, JAVELIN (Mar. 6, 2019), https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt.

[11] *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*, IBM NEWSROOM (July 23, 2019), https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Feltfor-Years.

[12] *Examining the Current Data Security and Data Breach Notification Regulatory Regime*, Hearing Before the House Fin. Svcs. Subcomm. on Fin. Institutions and Consumer Credit at 2 (Feb. 14, 2018) (Statement of Kim M. Sponem), *available at* https://www.cuna.org/uploadedFiles/Advocacy/Actions/Comment_Calls,_Letters_and_Testimonies/2018/Testimonies/KimSponem_Testimony_February%2014%202018.pdf.

[13] Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CTR. (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

[14] Verizon Data Breach Report, *supra* note 5, at 2.

In addition to requiring security protections, this bill also takes the important step of expanding the definition of personal information. Biometric data, for example, clearly warrants additional protections. Biometric data is commonly used to confirm consumers' identity and can easily be exploited for identity theft and fraud purposes. Unlike a credit card number, the consumer's biometric information cannot be changed in the event of a breach, making its unauthorized disclosure all the more dangerous. But concerns about its disclosure go far beyond its potential misuse for the purposes of fraud. Aside from the inherent privacy interest in keeping this information secure, the disclosure of biometric data—for example, of voice recordings—could lead to reputational or emotional harm. In light of the plethora of data breaches in recent years, biometric data should have these additional protections.

The bill also extends protections to DNA data. There are few legal requirements on companies collecting DNA, and given the increased collection of this data through sites such as 23andMe, at the very least, companies should be required to keep it secure. Companies need these incentives to protect this data: the DNA testing service Vitagene recently revealed that it left information derived from DNA data, including gene-based health information, unsecured on a server for years.[15] And in 2018, the ancestry site MyHeritage, which collects DNA data, disclosed that they left email addresses and hashed passwords unprotected on a server.[16] Breaches of this type of data can have devastating consequences: thieves could demand a ransom for the data, or it could be sold to insurance companies seeking to making important decisions about consumers.[17]

---

[15] Nico Grant, *DNA Test Service Exposed Thousands of Client Records Online*, BLOOMBERG (July 9, 2019), https://www.bloomberg.com/news/articles/2019-07-09/dna-testing-service-exposed-thousands-of-customer-records-online.

[16] Makena Kelly, *MyHeritage breach leaks millions of account details*, THE VERGE (June 5, 2018), https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach.

[17] Angela Chen, *Why a DNA data breach is much worse than a credit card leak,* THE VERGE (June 6, 2018), https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics.

Covering taxpayer identification numbers, as well, will help prevent tax identity theft, which occurs when thieves use consumers' identifying information to obtain tax refunds. This is a serious problem: in 2017, Americans lost an estimated $1.6 billion to tax ID fraud.[18] This bill also bridges an important gap by protecting passport information. The 2018 Marriott data breach, in which the passport information of over 5 million people was disclosed, highlights the need for greater security of government-issued identification.[19] Passport information, combined with other data, can be used to impersonate consumers online, making them more vulnerable to fraud.[20]

This bill expands protections with respect to notification by requiring companies to provide consumers with meaningful information about the information that was breached and how to respond. For consumers, notice of a data breach is necessary so that they can protect themselves from identity theft or other harms. Knowing what data was exposed can guide consumers in choosing which steps, in addition to security freezes and credit monitoring, they must take to avert additional forms of identity theft, such as medical or tax fraud. Consumers consistently reported after the Equifax data breach that they were frustrated by the confusing and unhelpful information that Equifax provided to them following the incident. This bill will help ensure that consumers get the information they need to respond effectively.

The bill will also benefit consumers by requiring companies to provide free credit monitoring for two years following breaches of an SSN or taxpayer identification number. Many companies profit handsomely from using consumer data, but they offer consumers little or no

---

[18] Joe Davidson, *Thieves targeted $12 billion through IRS tax fraud,* WASH. POST (Oct. 19, 2018), https://www.washingtonpost.com/politics/2018/10/19/thieves-targeted-billion-through-irs-tax-fraud/. https://www.irs.gov/newsroom/writtentestimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operationsapril-6-2017.

[19] Peter Holly, *Marriott: Hackers accessed more than 5 million passport numbers during November's massive data breach*, WASH. POST (Jan. 4, 2019), https://www.washingtonpost.com/technology/2019/01/04/marriott-hackers-accessed-more-than-million-passport-numbers-during-novembers-massive-data-breach.

[20] Laura Hautala, *Marriott breach: What to do when hackers steal your passport number*, CNET (Dec. 3, 2018), https://www.cnet.com/news/marriott-breach-what-to-do-when-hackers-steal-your-passport-number/.

recourse for data lapses. This remedy will help incentivize companies keep data secure and will offer to consumer some redress following a breach. While credit monitoring provides less protection than a credit freeze—which are now free under federal law[21]—it does provide useful and immediate information that could be used to limit the consequences of identity theft after the fact.

While this bill takes key steps to protect consumer data, it should be strengthened to help avoid any unintentional gaps in coverage. For example, while we appreciate that this bill expands protections to cover email accounts, covering all online accounts would better ensure that sensitive information that, once disclosed, could cause reputational or other harm, is covered. Further, the data security requirement should be expanded to cover certain data that may not necessarily trigger consumer notification. For example, companies should be required to keep behavioral data, search history, and shopping history secure, as it can reveal more about consumers than they might want to share with others: their sexual preferences, health issues, and political activities. In addition, the bill defines medical information to be about a consumer's medical or mental health treatment or diagnosis. This could inadvertently leave out dental information, or create a loophole for oral care providers, and should be modified to explicitly include oral health treatment. Finally, there may be overlap in subsection (IV) "biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as … genetic print: and subsection (VI) "Genetic information and deoxyribonucleic acid profile," leaving the difference between the two subject to interpretation; we suggest further refinement to clearly distinguish the two in order to avoid any unintended future interpretation.

[21] U.S. Code § 1681(i).

We look forward to working with the author to perfect the bill as it moves through the legislative process.

Finally, while expanding data security and breach notification requirements is real progress for consumers, this bill does not limit how companies obtain, share, and retain data in the first place. Fundamentally consumers need legislation that limits commercial collection and retention to what is reasonably necessary to provide services to consumers. Several states are considering data privacy laws in the wake of California's first-in-the-nation privacy law—the California Consumer Privacy Act (or CCPA)[22]—that gives consumers the ability to delete extraneous data held by companies and opt out of the sale of their information. Previously, we supported legislation before the Council that limited internet service providers' ability to monitor and sell data about customers;[23] similar legislation was passed last year in Maine.[24] We strongly urge the Council to take up data privacy legislation, and Consumer Reports would be happy to assist the Council in any way possible toward extending DC residents these protections.

Councilmembers have a unique opportunity to guarantee basic security protections with respect to consumer data. For too long, inadequate laws have allowed companies to collect and profit from the use of consumers' personal information without consumers' knowledge or control, and without the incentives to properly steward that information and protect it from criminals. Given the unprecedented level of data collection in today's marketplace, and emergence of new privacy threats every day, now is the time to ensure that DC residents have the data protections they deserve. We thank you for your work to address these vital consumer protection issues.

[22] Cal. Civ. Code § 1798.100 et seq.
[23] B22-0403 (2017).
[24] Maine 2019 SB 275.