Statement of Alan Butler

Executive Director, Electronic Privacy Information Center (EPIC)

Hearing on "Safeguarding Americans' Communications: Strengthening Cybersecurity in the Digital Era"

Before the

House Committee on Energy & Commerce

Subcommittee on Communications and Technology
United States House of Representatives

January 11, 2024

I. Introduction

Chair Latta, Chair Rogers, Ranking Member Matsui, Ranking Member Pallone, and Members of the Subcommittee, thank you for holding this hearing and for the opportunity to testify today on Safeguarding Americans' Communications. My name is Alan Butler, Executive Director at the Electronic Privacy Information Center. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to secure the right to privacy for all online in the digital age.

Communications systems are the backbone of Americans' daily lives. They are repositories of our most sensitive records and hold the keys to sensitive financial, administrative, business, and government networks. That is why communications systems are frequently targeted by malicious actors and why cybersecurity vulnerabilities in these systems are especially dangerous. Communications infrastructure is frequently targeted by foreign actors seeking to gain access to sensitive government and corporate information systems; by criminals seeking to harvest our credentials and steal our identities; and by individuals seeking to abuse others through direct control or to punish others through indirect exposure of personal information that puts the intended victim at increased risk of physical harm. Securing our communications data and networks is essential to defend our national security, to protect consumers, and to ensure public safety.

We are encouraged by this Subcommittee's efforts to safeguard Americans' private communications data and to strengthen our cybersecurity posture. And we believe that the Subcommittee should focus special attention on four areas of work that can help to make these systems more resilient and secure:

1. **Enact a strong and comprehensive privacy and data security law.**

An essential step to increase cybersecurity is to enact a strong, comprehensive federal privacy law that establishes both data minimization and data security protections. Members of this Subcommittee made progress toward that goal when you voted overwhelmingly in favor of the American Privacy and Data Protection Act. We urge you to continue that work; minimizing collection and retention of sensitive data will preserve privacy and improve cybersecurity.

2. **Support agencies charged with implementing and enforcing privacy and data security standards.**

It is critical that the agencies charged with setting and enforcing data protection standards are given the tools, resources, and authorities they need to keep our communications systems secure. We have seen over the last two decades that privacy and data security rules are not effective without robust enforcement and ongoing oversight. And the evolving nature of the threats and of vulnerable systems requires a nimble and proactive approach.

3. **Promote implementation of the third pillar of the National Cybersecurity Plan to "shape market forces to drive security and resilience."**

Incentives should be properly aligned to enhance security practices while preserving innovation and competition. The National Cybersecurity Strategy underscores we must ensure that responsibility for poor cybersecurity is born by entities best positioned to reduce risk.

4. **Prioritize improvements of core standards and protocols necessary to secure IoT systems and protect our communications infrastructure.**

Many of the cybersecurity threats that we face are exacerbated by the insecure IoT devices and by legacy systems that need to be updated. This is an infrastructure problem that should be prioritized by agencies within this Subcommittee's jurisdiction and deserves substantial investment of time, research, and other resources. Several areas of focus are called out specifically in the National Cybersecurity Strategy.

II. Our communications systems are under relentless threat from cyberattacks.

Our defenses against cyber threats cannot improve if we are in denial about just how deficient our current measures are and how these deficiencies have grown more severe over time. As many as half of US consumers have been affected by data breaches because a company holding their personal information was hacked. That is significantly higher than the global average of just 33 percent of consumers.[1] Even if the focus is narrowed solely to breaches of phone subscriber data, there have been millions of breaches impacting subscriber records just since January 2023; it is clear that urgent action is required.[2]

As the National Cybersecurity Strategy emphasizes, the "[c]ontinued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience."[3] The failure to implement necessary data security protections fuels systemic insecurity; when "organizations that have data on individuals fail to act as responsible stewards for this data, they

---

[1] *See* Prof. Carsten Maple, *2022 Consumer Digital Trust Index: Exploring Consumer Trust in a Digital World* 9 (2022), available at https://cpl.thalesgroup.com/resources/encryption/consumer-digital-trust-index-report.

[2] *See, e.g.*, Ionut Arghire, *Millions of AT&T Customers Notified of Data Breach at Third-Party Vendor*, Security Week (Mar. 10, 2023), https://www.securityweek.com/millions-of-att-customers-notified-of-data-breach-at-third-party-vendor/ (approximately 9 million subscribers impacted); @TomKemp00, Twitter (Mar. 6, 2023 10:12 PM), https://twitter.com/TomKemp00/status/1632942381380276226 (noting that account number, first name, phone number, email address, number of lines and basic devices (e.g. iPhone 7) on the account, installment agreement information, and in some instances rate plan name, past due amount, monthly payment amount, various monthly charges, and/or minutes used); Brian Krebs, *Hackers Claim They Breached T-Mobile More Than 100 Times in 2022*, Krebs on Security (Feb. 28, 2023), https://krebsonsecurity.com/2023/02/hackers-claim-they-breached-t-mobile-more-than-100-times-in-2022/; *Verizon Customer Data for Sale on Dark Web, New Data Breach Suspected*, https://thecyberexpress.com/verizon-customer-data-for-sale-on-dark-web/amp/ (breach of database of more than 7 million Verizon customer records revealed in January 2023, the second breach within twelve months).

[3] The White House, *National Cybersecurity Strategy* 19 (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

externalize the costs onto everyday Americans."[4] Companies are simply not investing adequately in data security and resiliency. One recent study of the cybersecurity workforce found numerous deficiencies resulting from inadequate staffing, including patching vulnerabilities in a timely fashion, engaging in ongoing risk assessment and management, and training employees.[5]

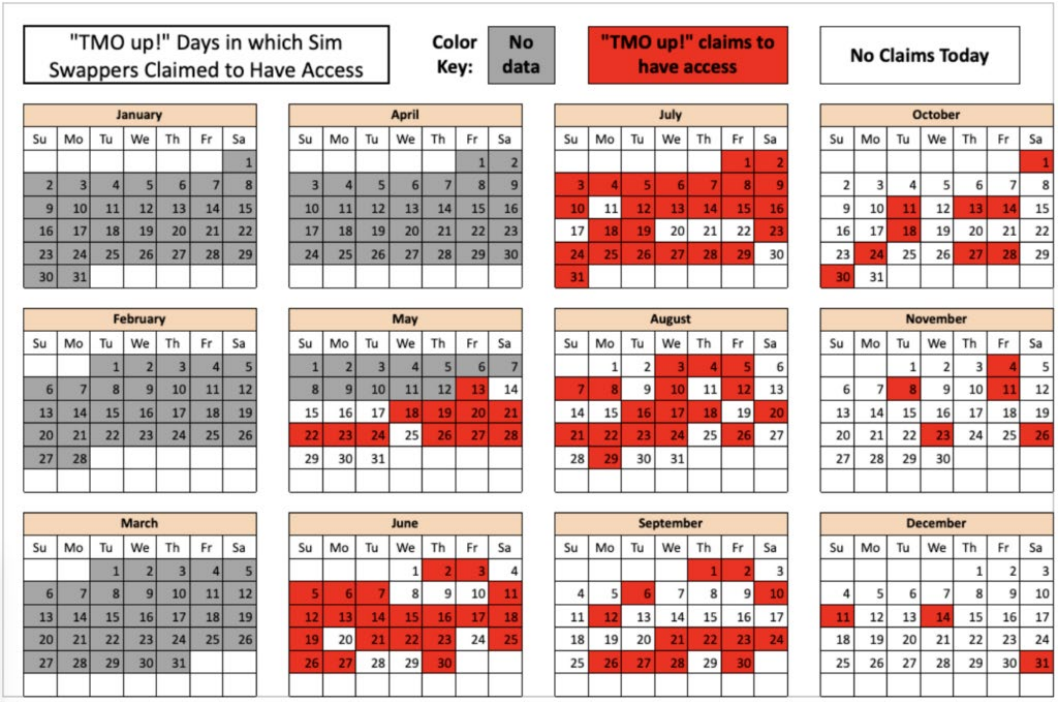
The risks created by inadequate investment in the administrative, technical, and physical procedures necessary to secure data against unauthorized access and acquisition are particularly acute in communications systems. We can update our passwords if they are compromised, we can replace our credit cards if they are stolen, but if our phone or e-mail accounts are seized then we are uniquely vulnerable, and it can be very difficult to recover. Even though traditional SMS-based text messages are one of the most widely used communications systems, they are incredibly vulnerable to *redirection attacks*.[6] In a redirection attack, a malicious actor can receive messages that were meant for a victim, including authentication codes or password reset links.[7]

These vulnerabilities have a widespread negative impact on cybersecurity because core security services are built on top of SMS—most notably "account validation, anomaly reporting, and one-time passwords (OTPs) for two-factor authentication."[8] For example, in 2019 Motherboard reported that vulnerabilities in SS7, the insecure messaging protocol that underlies SMS, was used "to target bank accounts by intercepting SMS text messages used as 2-Factor

---

[4] *Id.*
[5] *See* (ISC)[2], *Cybersecurity Workforce Study 2022* 10 (2022), https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.
[6] *See* Christian Peeters, et al., *SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication*, 22 Procs ASIA CCS 2 (2022), https://dl.acm.org/doi/pdf/10.1145/3488932.3497756.
[7] Mitchell Clark, *Companies Can Silently Reroute Your Texts to Hackers, Sometimes for Just $16*, The Verge (Mar. 15, 2021), https://www.theverge.com/2021/3/15/22332315/sms-redirect-flaw-exploit-text-message-hijacking-hacking.
[8] Peeters et al., *supra* note 6, at 2.

Authentication."[9] Similar attacks can be used to take control of cryptocurrency wallets or other financial accounts.[10] And these attacks have only become more prevalent. See, for example, a chart created by security researcher Brian Krebs, which shows in red the days on which known SIM-swapping groups advertised access to T-Mobile's employee tools (i.e., sold access to subscriber information only a carrier's employee should have):[11]



The calendar above (published on February 28, 2023) represents more than 100 days in 2022 during which bad actors were buying and selling unauthorized access to phone subscriber data at T-Mobile. The threat landscape has only gotten worse over the last year. In its most recent

[9] Joseph Cox, *Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts*, Motherboard (Jan. 31, 2019), https://www.vice.com/en/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank.

[10] *See* Thomas Brewster, *All That's Needed to Hack Gmail and Rob Bitcoin: A Name and A Phone Number*, Forbes (Sept. 18, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/?sh=dc3bda341a4f.

[11] Brian Krebs, *Hackers Claim They Breached T-Mobile More Than 100 Times in 2022*, Krebs on Security (Feb. 28, 2023), https://krebsonsecurity.com/2023/02/hackers-claim-they-breached-t-mobile-more-than-100-times-in-2022/.

quarterly report, the Identity Theft Resource Center observed a record-breaking 2,116 data breaches occurred in just the first three quarters of 2023.[12]

In many cases the security of our most sensitive accounts is reliant on the security of cell phone and e-mail systems that we rely on for secondary authorization and backup protection. That is why the security posture of communications companies demands special attention. The proprietary information of subscribers of each of the three largest carriers, for example, has been breached at least once within the last five years.[13]

Downstream consumer harms resulting from data breaches can include identity theft and other forms of account compromise. The Federal Trade Commission (FTC) reported in 2020 and in 2021 that credit card fraud and government documents or benefits fraud individually accounted for more than 27% of identity theft reports nationwide.[14] In 2023, the Department of Justice found that 59% of victims of identity theft suffered $1 or more in direct financial losses

---

[12] *See* Identity Theft Resource Center (ITRC), *Q3 2023 Data Breach Report: Identity Theft Resource Center Reports Data Compromise Record with Three Months Left in the Year* (Oct. 11, 2023), https://www.idtheftcenter.org/post/q3-2023-data-breach-report-itrc-reports-data-compromise-record-with-three-months-left-in-year/. This Q3 YTD figure of 2,116 compares with a total annual figure of 1,802 in 2022, *see ITRC Annual Data Breach Report* (Jan. 2023), available at https://www.idtheftcenter.org/publication/2022-data-breach-report/ ; *see also Record Number of Data Breaches in 2021*, IAPP Daily Dashboard (Jan. 25, 2022), https://iapp.org/news/a/record-number-of-data-breaches-in-2021/ (citing to ITRC report which estimated "1,862 breaches last year, up 68% from the year prior, and exceeded 2017's previous record of 1,506").

[13] *See*, *e.g.*, Lily Hay Newman, *T-Mobile's $150 Million Security Plan Isn't Cutting It*, Wired (Jan. 20, 2023), https://www.wired.com/story/tmobile-data-breach-again/; Brian Krebs, *It Might Be Our Data, But It's Not Our Breach*, KrebsOnSecurity (Aug. 11, 2022), https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/; Sergiu Gatlan, *Verizon notifies prepaid customers their accounts were breached*, Bleeping Computer (Oct. 18, 2022), https://www.bleepingcomputer.com/news/security/verizon-notifies-prepaid-customers-their-accounts-were-breached/.

[14] *See* FTC, *Consumer Sentinel Network: Data Book* 2020 at 9 (2021), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf (dividing number of reports by theft type by total identity theft reports).

with their most recent incident of identity theft,[15] and estimated that this fraud cost the U.S. economy more than $16 billion.[16] For example, in late 2020, websites used to generate auto insurance quotes were exploited to obtain personal data later used to submit fraudulent claims for pandemic and unemployment benefits.[17] Breached proprietary information could be used to similar ends.

The impacts of identity theft can be far-reaching, discovered only after downstream harms have occurred (e.g., through a collections notice for a bill the consumer never incurred nor knew of before receiving the notice), and difficult to remedy after the fact. A Government Accountability Office report indicated that past victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[18]

The FCC has stated that "[i]n the telecommunications industry, the public has suffered an increasing number of security breaches of customer information in recent years."[19] Some companies have argued that many incidents are the result of employee "accidents" and do not cause harm. But there is clear evidence of harm resulting from employee "accidents." Consumers are also at risk from the collection and sale or transfer of their sensitive data by communications

---

[15] *See* Bureau of Just. Stat., U.S. Dep't of Just., *Victims of Identity Theft, 2021* 8 (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf.
[16] *See id.* at 1 ($16.4BB in 2021); Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2018* 11 (Apr. 2020), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf ($15.1 billion in total financial losses due to identity theft where the victim lost $1 or more). This was also true in the DOJ's two prior reports. *See* Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2016* 1 (Jan. 2019), https://bjs.ojp.gov/content/pub/pdf/vit16.pdf ($17.5 billion); Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2014* 7 (Sept. 2015), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf ($15.4 billion).
[17] *See Industry Letter Re: Cyber Fraud Alert*, N.Y. State Dep't of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.
[18] U.S. Gov't Accountability Off., GAO-14-34, *Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent* 11 (2013), http://www.gao.gov/assets/660/659572.pdf.
[19] Fed. Commc'ns Comm'n, *In re* Data Breach Reporting Requirements, Notice of Proposed Rulemaking, WC Docket No. 22-21 at ¶ 1 (Jan. 6, 2023), https://docs.fcc.gov/public/attachments/FCC-22-102A1.pdf.

providers themselves (not malicious hackers). In October 2021, the FTC published a report that identified wide scale overcollection and transferring of sensitive browsing data by internet service providers (ISPs),[20] including both broadband and mobile providers (noting that several sold real-time location data derived from provision of their services to third-parties). In February 2020 the Federal Communications Commission (FCC) issued a Notice of Apparent Liability to major mobile carriers regarding their involvement in the illegal and dangerous sale[21] of consumer location information resulting in rogue law enforcement officers,[22] bounty hunters, and others obtaining real-time and historical location information. This sale was in violation of the FCC's rules[23] regarding Consumer Proprietary Network Information (CPNI), which includes when, for how long, and to/from whom a phone subscriber made or received a phone call. There has been no public announcement indicating that these fines have ever been collected by the FCC or by the U.S. Department of Justice.

There are clearly systemic data security problems in this industry that demand action.

---

[20] *See* Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* 34 (2021), *available at* https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major- internet-service-providers.

[21] Press Release, FCC *Proposes Over $200M in Fines for Wireless Location Data Violations*, Fed. Commc'ns Comm'n (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.

[22] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, The New York Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

[23] *See* Report and Order and Further Notice of Proposed Rulemaking, *In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, IP-Enabled Services, CC Dkt. No. 96-155, WC Dkt. No. 04-36 (Rel. Apr. 2, 2007), https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf.

III. It is essential that we enact a strong, comprehensive privacy and data protection law to strengthen cybersecurity and resilience.

Data protection and privacy should be a central focus of cybersecurity policy in the United States.[24] Enhanced privacy can result in enhanced security, just as weak privacy is likely to result in weak security. As Profs. Dan Solove and Woody Hartzog have outlined:

> There are several ways that bad privacy can lead to bad security: (1) Weak privacy controls can lead to improper access through the front door; (2) Collecting and storing unnecessary data can make data breaches much worse; (3) Poor privacy regulation can allow for more tools and practices that compromise security; and (4) A lack of accountability over data can increase the likelihood that the data will be lost, misplaced, or misused.[25]

One of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less personal information at the outset – a hacker can't gain access to data that a company does not have. Although it is not explicitly addressed in most cybersecurity regulations, data minimization is an accepted fundamental risk-reduction concept in cyber hygiene and information management.[26] Data minimization, paired with strong data

---

[24] *See* Eugenia Lostri and Stephanie Pell, *The Biden Administration's Implementation Plan for the National Cybersecurity Strategy*, Lawfare (Sept. 19, 2023), https://www.lawfaremedia.org/article/the-biden-administration-s-implementation-plan-for-the-national-cybersecurity-strategy (noting the recognition in the National Cybersecurity Strategy of "important relationship between data privacy and cybersecurity" and the need for a plan of action to achieve the goal of establishing comprehensive privacy and data security protections).

[25] *See* Daniel J. Solove & Woodrow Hartzog, *Breached! Why Data Security Law Fails and How to Improve It*, 143 (2022).

[26] *See, e.g.*, Fed. Trade Comm'n, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (advanced notice issued Aug. 22, 2022), https://www.federalregister.gov/d/2022-17752/p-88 (The term "data security" in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices); NIST SP 800-53-r5 at 72, 270; Federal Privacy Counsel, Fair Information Practice Principles (FIPPs), https://www.fpc.gov/resources/fipps/; 16 C.F.R. pts. 314.4(c)(6), 682; Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0 at 73-101 (Requirement 3) (March 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf. *See also* N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022); NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Apr. 16, 2018), at
34 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

security requirements, is the most effective way to protect against breaches and unauthorized access of personal data.

Data minimization sets limits on processing which requires data to be used *specifically* to deliver the goods and services that an individual has requested, consistent with the consumer's expectations.[27] Companies complying with data minimization requirements must also delete personal information when it is no longer needed to serve the purpose for which it was collected.

Section 101 of the American Data Privacy and Protection Act (ADPPA) introduced by Chair Rogers and Ranking Member Pallone last session set out a strong data minimization standard. It required that entities only collect, use, and transfer data that is *reasonably necessary* to provide a specific product or service requested by the individual with some enumerated exceptions. Particularly sensitive forms of data, such as location, communications, and financial data, warrant even stricter protection. The ADPPA recognized this, requiring that the collection and use of sensitive data be *strictly necessary* to provide the product or service requested. Often, these particularly sensitive types of data are most valuable to cyber criminals. Reducing the volume of sensitive data collected in the first place reduces the overall vulnerability by limiting the incentive for malicious actors to gain access. The adoption of data minimization techniques consistent with this rule is essential to data protection and cybersecurity.

The relationship between data security and data minimization is perhaps best summarized by the maxim "You don't have to protect what you don't collect."[28] Every piece of personal

---

[27] *See* John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, EPIC.org (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/; EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/.

[28] *Id.*

information collected and retained by a business is inherently at risk of unauthorized access and use. Technical and physical safeguards are certainly vital to limiting that risk, but one surefire strategy is for business to limit the data they collect and process in the first place. Practicing data minimization makes businesses less attractive targets for data thieves and hackers, limits the harm to consumers when breaches do occur, and fully eliminates the risk of breach for data elements that are never collected to begin with.

Data minimization is not a new concept; it just needs to be applied as a rule to all personal data collection online. Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[29]

The recently passed update to the California Consumer Privacy Act also includes provisions requiring a limited form of data minimization.[30] The European Union General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is "[a]dequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[31]

Ultimately, the best way to protect consumer data is to not collect, or not store, the data beyond what is reasonably necessary. Data that is never collected in the first place, or that is

---

[29] 5 U.S.C. § 552a (e)(1).
[30] Cal. Civ. Code § 1798.100(c).
[31] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

quickly deleted,[32] cannot be breached. The most important step Congress can take to strengthen cybersecurity is to enact a comprehensive privacy law with a strong data minimization rule as set forth in ADPPA.

IV. An effective cybersecurity regime requires a modern and nimble regulatory framework with robust enforcement to ensure there is a strong incentive to invest in secure systems and adopt necessary procedures.

Robust enforcement, more tailored cybersecurity standards, and new liability rules are necessary to shift market incentives to spur necessary investments in cybersecurity. Much of the work that needs to be done to bolster the security of our communications systems and of other parts of our critical infrastructure is laid out in the National Cybersecurity Strategy[33] and Implementation Plan.[34] Both this committee and federal agencies have focused significant attention on securing energy, transportation, and other critical systems given the risks to national security and public safety that could be caused by attacks on those systems. But more needs to be done to secure Americans' communications. The standards being developed for critical infrastructure security can and should inform cybersecurity standards for communications networks and services. Indeed, the Implementation Plan calls on NIST, CISA, and relevant "sector risk management agencies" (like the FCC) to "increase agency use of frameworks and international standards to inform regulatory alignment."[35] Ultimately, the Strategy calls for

---

[32] *See, e.g.*, 16 C.F.R. pts. 314.4(c)(6), 682; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022); NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* 34 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[33] The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy* (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.
[34] The White House, *National Cybersecurity Implementation Plan* (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.
[35] *Id.* at 13.

coordinated action across federal agencies and in collaboration with Congress to establish and implement minimum cybersecurity requirements and ensure that critical vulnerabilities don't fall through the gaps.[36]

The FCC, and other sector-specific agencies, must take a more active role in developing and enforcing cybersecurity standards under the Strategy and Implementation Plan. We cannot rely on market forces and industry self-regulation given the substantial risks that cybersecurity vulnerabilities pose to national security, public safety, and consumer wellbeing. Incentives need to shift to ensure that companies adequately invest in risk mitigation and in the secure-by-design innovations that can make our infrastructure more resilient. These incentives must effectively compel organizations to mitigate the costs of deficient cybersecurity that otherwise become externalized onto consumers, onto our national security, and by extension onto our economy. This incentive structure can be best achieved through a robust regulatory enforcement apparatus, through increased private sector accountability via no-fault liability underwritten by cyber insurance, or (ideally) a combination of both.[37] Clearer standards can help reduce uncertainty about what is expected of an organization's cybersecurity program, which in turn can ensure that resources are directed to manage risks most effectively.

As part of the Implementation Plan, the Office of National Cyber Director has already begun a review of potential ways to harmonize cybersecurity requirements across different sectors. This is an important opportunity that warrants close attention and participation by the

---

[36] *See id.*

[37] Treasury, following up on a GAO Report, has already begun to investigate how to prevent catastrophic cyber incidents pushing the insurance market beyond its capacity. *See* Treasury Dep't, Potential Federal Insurance response to Catastrophic Cyber Incidents, 87 Fed. Reg. 59,161 (Sept. 29, 2022), https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents.

FCC and other sector-specific agencies. In comments filed jointly in the harmonization inquiry, EPIC and Consumer Reports urged ONCD[38] to identify in its report the cybersecurity measures around which there is already consensus or near-consensus across different frameworks. [39] We believe there is already consensus or near-consensus on standards for: data minimization, heightened measures for high-risk activities, governance, data mapping, access controls, segmentation of systems, vulnerability management, threat detection, incident response, and business continuity.

There is striking similarity across multiple state laws, federal sectoral laws, agency enforcement actions, and both government and non-government frameworks regarding basic modern cybersecurity hygiene.[40] We have seen industry representatives argue that these frameworks, including the framework developed by NIST is not a "standard" that they must follow, but there is no evidence that requiring adherence to these frameworks is unreasonable or unfeasible.[41] Indeed, major communications carriers have acknowledged that the Tier 2 level of

---

[38] *See* Comments of EPIC and Consumer Reports*, In re* Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, ONCD-2023-0001-0028 (Oct. 2023), available at https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/.

[39] Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM- comments-Nov2022.pdf; *see also* Comments of the Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America, to the California Privacy Protection Agency, Proceeding No. 02-23 at Appendix 1 (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/.

[40] *See, e.g.,* Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 194-197 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM- comments-Nov2022.pdf.

[41] *See, e.g.*, *in re* Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Comments of Verizon, IB Docket No. 23-119, at 21-22 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108312266504640; Comments of CTIA at 52 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108311863500689; Comments of T-Mobile at 22-23 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831234137677.

the latest version of NIST's Cybersecurity Framework (CSF) "provides an appropriate baseline" standard.[42] Leaders at key federal agencies should (re)set expectations with industry regarding their responsibility to safeguard consumer information from unauthorized access, follow up on the guidance issued from California's Department of Justice in 2016[43], from the FTC in 2015,[44] and from the White House in 2021,[45] and invest the resources necessary to bring companies into compliance.

Establishing strong, comprehensive privacy and data security standards will help to properly align the incentives of businesses to better safeguard the personal data that they collect. These incentives can be created both through direct rules that set standards for data security and data minimization, and through more indirect means by establishing liability rules for cybersecurity deficiencies. Many courts have considered the assignment of liability under current

---

[42] Comments of Verizon, IB Docket No. 23-119, at 23. Verizon goes on to say that "[a] Tier 2 baseline implementation of the CSF would thus serve as a dynamic, discerning, and risk-based approach consistent with the 2023 National Cybersecurity Strategy and the government's approach to cybersecurity as discussed above." *Id.* at 24-25. *See also* Comments of USTelecom at 10 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831107732869.

[43] In a 2016 report on data breaches, then-California Attorney General Kamala Harris stated as her first recommendation: "[t]he 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet." Kamala D. Harris, Attorney General, California Data Breach Report 30 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf. That statement applied to the largest economy in the country and was made approximately seven years ago.

[44] The FTC has been offering explicit guidance on specific cybersecurity practices since at least as early as 2015. *See, e.g.*, Fed. Trade Comm'n, Start With Security: A Guide for Business (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

[45] *See* The White House, *What We Urge You To Do To Protect Against The Threat of Ransomware* (June 2, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf ("what we urge you to do now"). *See also* The White House, Fact Sheet: Act Now to Protect Against Potential Cyberattacks (Mar. 21, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/ ("we urge companies to execute the following steps with urgency").

state and common law principles, but clear rules are necessary to ensure that necessary precautions are taken.[46] That is why a uniform federal standard is so important.

One major consideration is whether a data security standard should impose no-fault liability or whether it should impose a per-se negligence or traditional negligence standard. The National Cybersecurity Strategy recognizes that "[r]esponsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product."[47] Many experts, including Professor Danielle Citron, have argued that data security incidents should be analyzed under the same strict liability tort standards that govern accidents involving hazardous materials.[48] This rule is in line with the long-recognized principle that the "least cost avoider" in an accident should be held responsible so that they are properly incentivized to take preventative measures to avoid the loss.[49] Although businesses may claim that they were the victims of sophisticated attackers,[50] if the business collects consumer data, it has taken on the responsibility of protecting that data, and it is liable when data in its custody is breached. Insurance can help to mitigate the cost of such

---

[46] *See, e.g.*, Br. of Amici Curiae Electronic Frontier Foundation and EPIC, No. 22-1744(L) (4th Cir. Nov. 22, 2022), https://epic.org/documents/peter-maldini-v-marriott-international-inc/ (data breach of hospitality company); Br. of Amici Curiae EPIC and National Consumers League, No. 23-55375 (9th Cir. Aug. 2, 2023), https://epic.org/documents/michael-terpin-v-att-mobility-llc/ (targeted cryptocurrency theft effectuated by bribed telecom carrier employee).
[47] *National Cybersecurity Strategy*, *supra* note 3 at 21.
[48] *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 Cal. L. Rev. 1805, 1844–48 (2010).
[49] *See* Guido Calabresi, *The Cost of Accidents: A Legal and Economic Analysis* 136–38 (1970) (applying the least cost avoider to a typical car accident scenario).
[50] *See, e.g.*, Microsoft Security Response Center, *Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server* (Sept. 29, 2022), https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/.

data security protocol failures, which in turn will limit the impact on cost to consumers.[51] A company is in control of what data it chooses to collect, how long it chooses to retain it, and when and how it decides to dispose of the data. A company is in control of what processes it uses to safeguard that data, including mitigating the harm in the event of a breach (e.g., segmenting systems). If a company collects consumer data, it accepts liability for what happens to that data until that data has been safely disposed of.

Overall, by shifting the liability for privacy and security onto product developers and service providers—as the White House strategy suggests—EPIC believes we will begin to see industry-wide changes that result in increased privacy protections and higher cybersecurity standards.

Although it is difficult to remedy the harms of identity theft after the fact, preventing the underlying breach is neither difficult nor expensive. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable;[52] and more recently the Internet

---

[51] Josephine Wolf, *Time for Regulators to Take Cyber Insurance Seriously*, Lawfare (Mar. 17, 2020), https://www.lawfareblog.com/time-regulators-take-cyber-insurance-seriously ("Organizations increasingly rely on cyber insurance to help manage online risks. It is time for regulators to stop treating this market as a small, peripheral piece of the insurance industry and instead focus their attention on how they can help transform it into a more stable and effective tool for cybersecurity risk management."); Cyber Insurance, FTC https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance ("Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. . . . Also, consider whether your cyber insurance provider will: Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)."). But insurance companies may need more information. *See, e.g.*, Cyberspace Solarium Comm'n, Final Report 79 (2020),https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf (recommendation 4.4).

[52] 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, Alert: Top 30 Targeted High Risk Vulnerabilities (2016), https://www.us-cert.gov/ncas/alerts/TA15-119A. The California AG's Office similarly concluded that many of the hundreds of breaches it studied could have been prevented, or detected and corrected more rapidly, by implementation of its recommended data security controls. *See* Kamala D. Harris, Attorney General, *California Data Breach Report* 32 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

Society has estimated 95 percent of breaches could have been prevented.[53] The FTC has often noted that reasonable security measures are a relatively low cost.[54] As renowned security technologist and fellow at Harvard Kennedy School Bruce Schneier observed in 2022:

> In all of these cases, the victimized organizations could have very likely protected our data better, but the reality is that the market does not reward healthy security. Often customers aren't even able to abandon companies with poor security practices, as many of them build "digital moats" to lock their users in. Customers don't abandon companies with poor security practices. Hits to the stock prices quickly recover. It's a classic market failure of a powerful few taking advantage of the many, and that failure is one that only representation through regulation can fix.[55]

Two professors at Antonin Scalia Law School have similarly argued, in a recent Michigan Technology Law Review article, that a strict liability regime would correct for the current failure of firms to internalize the cost and benefits of their data security decisions.[56] They further argue that the firm has incentives to take socially optimal security precautions—which will in turn lead

---

[53] Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* 3 (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.

[54] *See, e.g.*, Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter; Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 23 (Jan. 26, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc matter; Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 11 (Dec. 30, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc; Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 22 (Sept. 6, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter; Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶¶ 23(A)(iv), 24 (N.D. Ga. Jul. 22, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc; Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 42 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison; Complaint, In re Lenovo, Inc., FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc.

[55] Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, The New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html.

[56] *See* James C. Cooper & Bruce H. Kobayashi, Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem, 28 Mich. Tech. L. Rev. 257, 263–64 (2022), https://repository.law.umich.edu/mtlr/vol28/iss2/3.

to socially optimal data collection decisions—if a firm internalizes the harm,[57] and moreover that strict liability would facilitate cyber insurance calibrated to an optimal standard of care.[58]

This strongly suggests that the cost and harm to consumers and to the American economy (due to fraud facilitated by identity theft) that result from data breaches would be better internalized as preventative data security costs incurred by the carriers (and their partners and vendors), which are best positioned to prevent the harm from occurring in the first place.

Cyber insurance may itself also encourage better cyber security practices by companies.[59] For example, a survey of three cybersecurity insurance providers by the International Association of Privacy Professionals revealed common expectations of best practices, including firewalls, patching, passwords, and authentication, and noted that they may deny coverage if policyholders "do not exercise the degree of caution they promised in the underwriting process."[60]

The U.S. Department of the Treasury has also underscored the important risk-transfer function of cyber insurance, that insurance can play an important role in strengthening cyber hygiene and cybersecurity resiliency, and that the industry is growing, with more than $4 billion

---

[57] *See id.* at 287.
[58] *See id.* at 295.
[59] *See, e.g.*, U.S. Gov't Accountability Off., GAO-22-104256, Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks at 18-19, https://www.gao.gov/assets/gao-22-104256.pdf ("In addition to covering costs associated with common risks, cyber insurance can encourage policyholders to manage their cyber risk and increase cyber resilience, according to several government entities and researchers…. Some government entities and researchers also have noted that the insurance market can encourage implementation of cybersecurity best practices by linking premiums with the policyholder's cybersecurity practices", but noting that it may make companies more likely to pay ransomware demands which in turn may encourage more cyber attacks); William McGeveran, The Duty of Data Security, 103 Minn. L. Rev. 1135, 1171–72 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf ("Insurers can and do push their policyholders to adopt practices that reduce the insurer's risk of loss—and simultaneously promote better protection of personal data.").
[60] McGeveran at 1173.

in direct premiums written in 2020.[61] The Cybersecurity & Infrastructure Agency (CISA) notes that over the first half of 2018 the overall cyber insurance take-up rate was approximately 32%, with 75% of largest companies in key sectors purchasing some cyber insurance and fewer than 5% of small and medium businesses participating.[62] Although the industry is still comparatively young, it is growing quickly. And with good reason—in addition to data breaches in which privacy is violated and ransomware in which data or systems are made inaccessible, there are also the threats of leveraging devices to cause harm to other systems.[63] Companies are in the best position to protect consumers from these harms, and the insurance industry is catching up to the market scale that is needed, but companies must be adequately incentivized to change data security practices market-wide. While state data breach laws have been much maligned for the alleged patchwork they were said to create, it cannot be denied that they have incentivized

---

[61] *See, e.g.*, Treasury Dep't, *supra* note 37 at 59161–62 ("Through underwriting and pricing, insurers can encourage or even require policyholders to implement strong cybersecurity standards and controls."); Leslie Scism, Insurers Creating a Consumer Ratings Service for Cybersecurity Industry, Wall Street Journal (updated Mar. 26, 2019), https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600 ("Many insurers see the burgeoning cyber-risk market as a rare growth opportunity when many other insurance lines are growing sluggishly."); Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* at 7 (July 9, 2019) (noting that the cyber insurance market is showing signs of maturing).

[62] *See* CISA, Assessment of the Cyber Insurance Market 5 (Dec. 21, 2018), https://www.cisa.gov/sites/default/files/publications/20_0210_cisa_oce_cyber_insurance_market_assessment.pdf ("Aon Inpoint estimates that while 75 percent of financial institutions, retail, health care, and hospitality companies with revenue over $1 billion purchase some cyber insurance, fewer than 5 percent of small and medium businesses are consumers in the market.").

[63] *See, e.g.*, Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. Mich. J.L. Reform 913 (Apr. 20, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2955317 (describing how a botnet comprised of inadequately secured IoT devices was used to cause a Denial of Service attack in 2016, and articulating a theory of products liability for manufacturers of hacked devices, especially as these attacks have become highly foreseeable).

companies to report cyber incidents to impacted consumers and regulators more effectively than the absence of such laws.[64]

In addition to strengthening incentives through clear standards and liability rules, there is more work to be done to improve the standards for internal and external security reviews by companies themselves. An audit requirement alone will not result in meaningful protection if the audits measuring adherence are not both independent and thorough. For example, an audit should not merely report the audit subject's response as to whether the organization has a strong password policy in place; rather, the auditor should attempt to set up access with a weak password to see if the policy has been implemented and works as intended.[65] Twitter whistleblower Peter "Mudge" Zatko remarked in his 2022 Congressional testimony:

> [H]ow was Twitter still operating like this? Since there was a 2011 consent decree that was aimed at addressing a fair amount of this? . . . One, there were a lot of evaluations and examinations, which were interview questions. So essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn't a lot of ground truth. There wasn't a lot of quantified measurements. And a fair amount of the interviews came from companies, auditors that Twitter themselves were able to hire. So I think that's a little bit of a maybe conflict of interest.[66]

Mudge suggested the solution include "accountability, and setting quantitative goals and standards that can be measured and audited independently" in order to "change management structures, and drive change in companies when it's needed such as this."[67] We have urged regulators to establish quantitative goals and standards, requiring actual investigation and

---

[64] *See* McGeveran at 1152 (noting breach notification requirements have driven "a large proportion of corporate efforts to improve institutional data security").
[65] *See* Kevin G. Coleman, *Security Assessment or Security Audit?*, infoTECH Spotlight (Sept. 21, 2009), https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.
[66] Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022) (testimony of Peter Zatko), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower.
[67] *Id.*

analysis and not merely interviews.[68] We have also encouraged regulators to establish processes that reduce the likelihood of a conflict of interest as described in Mudge's testimony. Ultimately, an audit requirement will only be effective if the required audits are independent and thorough.[69] Unfortunately, false certifications about privacy and cybersecurity compliance are a known issue. The Department of Justice has set up an entire initiative to address this issue with federal contractors.[70] Verizon has reported in the payment security context that most organizations fail to maintain compliance between annual compliance validations.[71] Ensuring that regulatory agencies have the resources necessary to bring enforcement actions against entities filing false or deficient certifications will also be critical to achieving our cybersecurity goals.

V. The proliferation of IoT devices warrants special attention but efforts to shield manufacturers from liability miss the mark.

Many of the cybersecurity threats that we face are exacerbated by insecure Internet of Things ("IoT") devices and by legacy systems that need to be updated. This is an infrastructure problem that should be prioritized by agencies within this Subcommittee's jurisdiction and deserves substantial investment of time, research, and other resources. Americans are rightly

---

[68] We urge regulators to state explicitly that a certification is deficient if the company's audit was based solely on staff interviews and did not entail any actual testing of whether the safeguards are operating as intended.

[69] *See, e.g.,* Draft Cybersecurity Audit Regulations for California Privacy Protection Agency (CPPA) Sept. 8, 2023, Board Meeting, at 7-9 Section 7122, available at https://cppa.ca.gov/meetings/materials/20230908item8.pdf.

[70] *See, e.g.*, Press Release, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative; Madison Alder, Verizon agrees to settle False Claims allegations over cyber standards for federal contractors, FedScoop, (Sept. 5, 2023), https://fedscoop.com/verizon-to-settle-cyber-false-claims-allegations/.

[71] *See* Verizon, 2022 Payment Security Report 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf (Verizon consistently reports that 44 percent or more of organizations fail to maintain PCI- DSS compliance in between annual compliance validations, most recently more than 56 percent failed to maintain compliance).

concerned about what information their devices may be collecting about them and their family, and businesses would be wise to learn from the past and invest now in developing secure data privacy and security systems to avoid future breaches, suits, and a fragmented, reactive regulatory response. The National Cybersecurity Strategy specifically identifies the development of secure IoT devices as a key strategic objective, but the plan to carry out that objective is still being developed.

The FCC has proposed a cybersecurity labeling program that represents a first step on the path towards that secure IoT goal.[72] A key component of this strategy aims to expand IoT security labels, empowering consumers to make informed comparisons and ultimately "[create] a market incentive for greater security across the entire IoT ecosystem."[73] We recommend that any labelling standard include provisions that empower consumers and consumer advocates to have easy access to information about what data is being collected about them and how that data is being used, stored, or transferred. And we recommend against any system that further insulates companies from liability for insecure devices; the National Cybersecurity Strategy makes clear that there is clear need for more, not less, exposure to the downstream risks that insecure systems are creating for (and costs they are imposing on) consumers.

Given the label's primary goal of ensuring consumer confidence in the cybersecurity of their IoT devices, we believe that the FCC should adopt a dual-layer labeling solution. This solution would include an easily glanceable primary label and a secondary label that displays additional cybersecurity and privacy information, empowering consumers to make an informed

---

[72] *See National Cybersecurity Strategy supra* note 3 at 20.
[73] *See id.*; *see also* Fed. Commc'ns Comm'n, Cybersecurity Labeling for Internet of Things, Notice of Proposed Rulemaking, 88 Fed. Reg. 65937 (Aug. 25, 2023), https://www.federalregister.gov/documents/2023/08/25/2023-18357/cybersecurity-labeling-for-internet-of-things.

purchase at point of sale. For most products, we supported the FCC's proposal that the product itself contain a mark–a "U.S. Cyber Trust Mark." To qualify for the U.S. Cyber Trust Mark, our proposal would require data minimization, where the product itself to collect only the data necessary to provide its essential functions and services. Companies should design the product itself to include the mark. Additionally, the product box should include a primary label which displays information most critical to the consumer's evaluation of the product's relative cybersecurity, including the kind of data the device collects (e.g. video, audio, physiological, geolocation, etc.) per Carnegie Mellon University CyLab's model.[74] The primary label on the product box should also include a URL and a QR code to connect the consumer to a website which hosts a secondary label that displays a set of more detailed information regarding the privacy and cybersecurity of the device.

To help remedy consumer harms, we have also recommended that the FCC consider implementing a "cure period" for non-compliant companies to fix discovered vulnerabilities. A cure period gives good actors the opportunity to fix any issues without incurring penalties and ultimately ensures more protection of consumer data.[75] An IoT device breach can compromise security cameras, enabling thieves to effectively break into locations, enable blackmailers to

---

[74] *See* Ryan Noone, CyLab presents IoT privacy and security label research at White House summit, CyLab (Oct. 19, 2022), https://www.cylab.cmu.edu/news/2022/10/19-cylab-presents-at-white-house-iot-security-summit.html.

[75] The longer a vulnerability remains unpatched, the more likely that a bad actor will be able to exploit it. Allowing a short cure period will incentivize companies to fix vulnerabilities quickly, giving less opportunities for exploitation. As noted by Consumer Reports, other Federal agencies follow this rationale in requiring prompt cybersecurity incident disclosures. *See* Consumer Reports, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things, PS Dkt. No. 23-239 at 31 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/100623134834 (*citing* U.S. Securities and Exchange Commission, *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (last accessed Oct. 6, 2023), https://www.sec.gov/news/press-release/2023-139).

harass individuals with material from the individual's personal security cameras, and other irrevocable privacy-related harms.[76] Furthermore, this type of breach could also negatively impact national security, like when location data from a popular fitness app exposed the location of secret U.S. military bases.[77] As explained in the National Cybersecurity Strategy, insufficient IoT device security can cause incredible harm, and oversight mechanisms should reflect this severity.[78]

We have opposed proposals by device manufactures in the FCC Cyber Trust Mark rulemaking for a safe harbor that would provide a shield against liability for insecure devices. A safe harbor provision would directly contradict the National Cybersecurity Strategy as well as consumer expectations, and allowing self-certification would further contradict both. Ultimately, the goal of the proposed label is to help increase consumer confidence in the cybersecurity capabilities of their IoT devices. A safe harbor provision would place undue weight on a voluntary labeling program. Not only would a breach involving a product carrying the label shake consumer trust in the label; the availability of a "safe harbor" would fail to incentivize companies to keep their products safe and secure. The safe harbor would also disincentivize timely reporting of breaches, as companies are required to timely report breaches regardless of

---

[76] *See* Mike Elgan, *IoT Security: Thieves Are Targeting Smart Cameras – Here's How To Stop Them*, SecurityIntelligence (June 3, 2021), https://securityintelligence.com/articles/iot-security-smart-camera-thieves/.

[77] *See* Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, The Guardian (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-arm y-bases.

[78] *See National Cybersecurity Strategy*, *supra* note 3, at 2–4. *See also* Statement of Commissioner Nathan Simington, Federal Communications Commission, https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-devices/simington-statement. Harms can be economic, from identity theft to industrial sabotage, or can even be physical, as in the case of hacks of medical devices.

culpability.[79] Data breach reporting is typically strict liability – regardless of fault, if a breach occurs, a company is required to report that to both regulators and affected consumers.[80]

Furthermore, a formal safe harbor program may not actually be a useful defense in litigation. While approval to use the cybersecurity label would be relevant in determining whether a company's cybersecurity practices were reasonable, the company would still need to prove that they were in compliance with the program in order to take advantage of such a defense.[81] It is possible that a company approved to use the label but would not in fact be in compliance with its obligations; that company should not be able to avoid liability through its mere participation in the labeling program.

Noncompliance with label obligations may come to light during a cybersecurity incident. In these cases, consumers are likely to view insulation from liability with skepticism and distrust. They are not likely to see previous years of compliance as a sufficient basis to excuse current negligence, and any safe harbor provision may contribute to this perception in the public eye. If that comes to pass, the label will fail at one of its most basic goals: ensuring consumer confidence in the cybersecurity of their devices.

VI. Conclusion

Securing our nation's communications systems is essential to protect national security, public safety, consumers, and our economy. This Subcommittee has the opportunity to promote important legislation to establish privacy and data security protections that are desperately needed across the digital ecosystem. And there is a range of other important work ahead to implement the National Security strategy and develop strong cybersecurity standards, to properly

---

[79] *See, e.g.*, Consumer Reports Comment Letter, *supra* note 75, at 38–39.
[80] *See id.*
[81] *See id*.

align industry incentives to invest in robust cybersecurity practices, and to better secure the devices and systems that play such an essential role in our day-to-day lives.

Thank you for the opportunity to testify today.