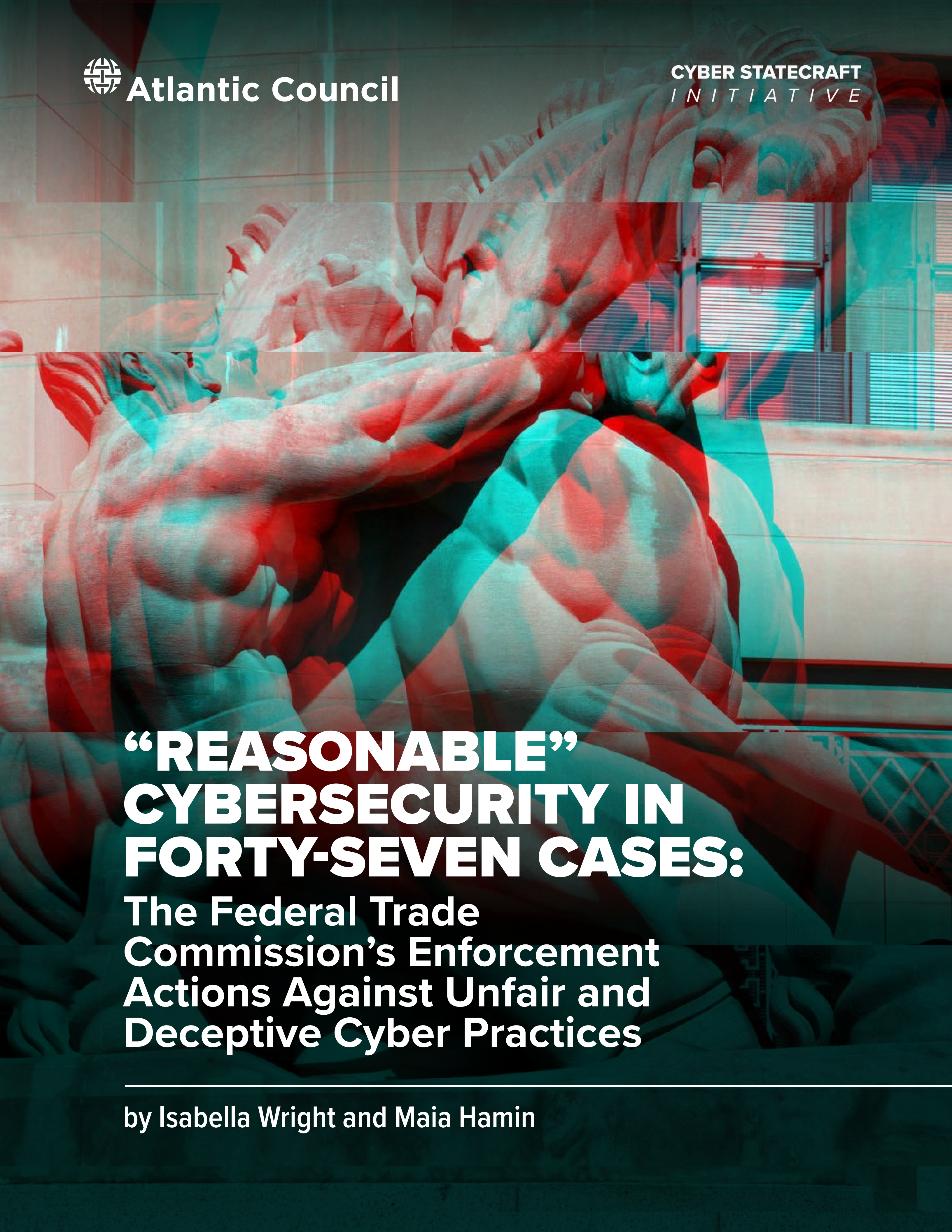
Atlantic Council

CYBER STATECRAFT INITIATIVE



“REASONABLE” CYBERSECURITY IN FORTY-SEVEN CASES:

The Federal Trade Commission’s Enforcement Actions Against Unfair and Deceptive Cyber Practices

by Isabella Wright and Maia Hamin

Atlantic Council

CYBER STATECRAFT INITIATIVE

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Authors

Isabella Wright
Maia Hamin

Editor

Samia Yakub

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

June 2024

Design by: Donald Partyka

Cover: Highsmith, Carol M, photographer. "One is Man Controlling Trade,"statue by Michael Lantz, at Federal Trade Commission, 600 Pennsylvania Ave., NW Washington, D.C. United States Washington D.C. District of Columbia Washington D.C, 2010. Photograph. https://www.loc.gov/item/2010641732/.

Atlantic Council

CYBER STATECRAFT
INITIATIVE

“REASONABLE” CYBERSECURITY IN FORTY-SEVEN CASES:

The Federal Trade Commission’s Enforcement Actions Against Unfair and Deceptive Cyber Practices

by Isabella Wright and Maia Hamin

Table Of Contents

Acknowledgements

Thank you to Josephine Wolff, Natalie Thompson, Chris Hoofnagle, Stew Scott, and Trey Herr for feedback and suggestions on various versions of this document—it is far stronger for it. Thank you to the policymakers and researchers who spoke with us in conversations on background to inform this work. And, finally, thank you to Nancy Messieh, whose built the interactive visuals that substantially enrich this document's analysis.

Executive Summary

The Federal Trade Commission (FTC) is a small US government agency whose consumer protection remit is increasingly the starting point to govern the design and operation of a multitude of impactful digital products and services. In the absence of either a comprehensive, federal-level consumer privacy or data security law in the US, the FTC has used its legal authority to police "unfair and deceptive acts and practices"[1] in commerce to become the lead federal enforcer for the privacy and security of consumer data.

This report provides a historical examination of forty-seven FTC enforcement actions related to unfair and deceptive acts and practices related to cybersecurity from 2002 to 2024, including the cybersecurity practices (or lack thereof) that caused the FTC to pursue each case and the requirements it placed upon companies to establish a comprehensive information security program in response. This analysis reveals how the FTC, armed with a mandate from 1914, has effectively constructed a body of "reasonable" cybersecurity practices and clear precedent for their enforcement.

Throughout these cases, the FTC's central identity as a consumer protection agency is clear. The commission's cyber enforcement, in part due to the scope of its authorities, has focused heavily on addressing instances of insecurity that drive harm, whether due to the volume or nature of consumer data at risk. The FTC has levied complaints against companies of all shapes and sizes for an equally diverse range of security bad practices, from allowing users to share credentials to failing to monitor technical vulnerability reports. Many of these complaints hinge on questions of "reasonable" cyber practices to protect consumers from harm or to uphold promises made in privacy policies and similar; thus, compiling the complaints begins to illuminate a body of baseline reasonable cybersecurity practices, as well as illustrate the persistence, over twenty years, of certain unsafe practices.

Over most of the last two decades, the agency's language for consent decrees—agreements that prescribe corrective actions that must be undertaken by the companies that agree to them—changed little between cases, despite the diversity of companies and practices that these decrees addressed. This trend changed following a 2019 ruling from the Eleventh Circuit that the FTC's data security consent decree against LabMD was "unenforceabley vague."[2] Since then, consent decrees have become more specific and tailored to the security failures that instigated the FTC's complaint. Yet, even these new decrees illustrate the ways in which the FTC's consent decrees combine both general and specific obligations to build requirements that can endure across the changes in technology and security practice that inevitably occur during a consent decree's twenty-year lifetime.

This paper reviews these trends from these forty-seven cases in light of recent policy debates over resolving persistent cyber insecurity, including the Biden administration's 2023 proposal to implement liability for vendors of insecure software[3] and recent proposals to codify data security standards as part of a federal consumer privacy law.[4] Many of these debates involve questions of how to define good and bad behavior with respect to cybersecurity and how to balance specificity and adaptability in the design of such frameworks. Studying the standards embedded within the "common law"[5] for consumer data security that the FTC has built through its cases offers an immediately useful foundation for the creation of cyber standards in the software liability context and beyond.

This analysis also illustrates some of the challenges with this model— the FTC as the stopgap federal enforcer for consumer cybersecurity—not least of which is the fact that the agency has had only forty-seven cases in which to articulate reasonable practices for twenty years' worth of blistering technological and commercial progress in consumer technology. The arrow of change in digital technology points toward yet wider dependence on common architectures and broadly adopted platforms, so, the paper briefly concludes with consideration of whether and how the FTC and future cyber policy mechanisms can adapt to meet this challenge.

[1] Federal Trade Commission Act of 1914, § 5, 15 U.S.C. § 45 (1914).

[2] LabMD, Inc v. Federal Trade Commission, 16-16270 (11th Cir 2018).

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

[4] US Congress, *American Privacy Rights Act of 2024 Discussion Draft*, https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf.

[5] Woodrow Hartzog and Daniel J. Solove argue for the use of this term to describe the FTC's case precedents; see Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," Columbia Law Review (2014), 583.

Introduction

Despite the growing importance of computing technology and the increasing sensitivity of the data collected by myriad systems from social media websites to wearable tech, the United State lacks a federal regulator with the explicit authority to set baseline cybersecurity standards for systems that hold and process sensitive consumer data.

With no singular federal data security regime in place, legal cybersecurity requirements have come from a patchwork of alternate sources including state-level privacy laws, sector-specific privacy and security rules, reporting requirements, and cybersecurity standards for government contractors.[6] Many states have passed privacy laws that often include requirements for companies processing personal data to abide by certain cybersecurity standards.[7] At the federal level, both the healthcare and financial sectors are subject to specific regimes governing privacy and data security—the Health Insurance Portability and Accountability Act (HIPAA)[8] and the Gramm-Leach Bliley Act (GLBA).[9] The FTC dictates cybersecurity protections for certain types of data under these laws as well others under the Fair Credit Reporting Act (FCRA)[10] and the Children's Online Privacy Protection Act (COPPA).[11] The Federal Communications Commission regulates "common carriers" such as telephone network providers; under the 2015 Open Internet Order, it designated broadband internet access providers as common carriers subject to Title II of the Telecommunications Act, requiring them to adopt new data protection and privacy rules (and excluding them from the FTC's jurisdiction).[12] Other federal entities regulate disclosures—not practices—relating to cyber incidents: the Securities and Exchange Commission (SEC) recently adopted rules requiring publicly traded companies to disclose material cybersecurity incidents for the benefit of their investors;[13] and the US Cybersecurity and Infrastructure Agency recently put out proposed rules to implement required reporting under the Cyber Incident Reporting for Critical Infrastructure Act.[14] Thus, different US federal enforcers have bitten off different pieces of the cybersecurity ecosystem, regulating specific types of data, technologies, or behaviors such as disclosures of cyber incidents.

For the consumer data and consumer technologies that remain, the main stopgap protection comes in the form of the FTC's consumer protection authority. Section 5a of the FTC Act grants the agency broad latitude to hold entities liable for "unfair and deceptive acts and practices" in commerce.[15] It is this authority that the FTC has used to become, in some sense, the United States' cyber regulator of last resort.

This report is concerned with the question of how the FTC has used this stopgap authority. What types of companies and failures has the agency prioritized? What practices or behaviors recur as drivers of insecurity in the consumer context? And, what lessons do the FTC's actions thus far offer for US policymakers considering how to establish a more comprehensive approach to consumer data security? The authors begin with an overview of the FTC itself and the authorities it has used to undertake this stopgap cyber oversight, as well as the nature of the complaints and consent decrees that are the legal tools through which this strategy is realized. Next, the report reviews the methods used to select and analyze the dataset of cases that underpins its analysis, and then presents the findings, identifying practices and remedies put forward by the FTC in the context of specific cases as well as high-level trends and themes that stretch across the cases. Finally, it extrapolates these findings into takeaways for policymakers seeking to design or refine mechanisms and authorities relating to cyber protections for consumers.

[6] Maia Hamin and Isabella Wright, "The U.S.'s FAR-Reaching New Cybersecurity Rules for Federal Contractors," *Lawfare,* February 1, 2024, https://www.lawfaremedia.org/article/the-u.s.-s-far-reaching-new-cybersecurity-rules-for-federal-contractors.

[7] " State Laws Related to Digital Privacy," National Conference of State Legislatures, accessed March 26, 2024, https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy.

[8] Health Insurance Portability and Accountability Act (HIPAA) of 1996, § 264a, 42 U.S.C. § 1320d-2 (1996).

[9] Financial Services Modernization Act of 1999, 15 U.S.C. § 6803 (1999).

[10] Fair Credit Reporting Act, 15 U.S.C. § 1681s (1970).

[11] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).

[12] Federal Communications Commission, "FCC Releases Open Internet Order," March 12, 2015, https://www.fcc.gov/document/fcc-releases-open-internet-order.

[13] Maia Hamin, "Who's Afraid of the SEC?," DFRLab, June 14, 2023, https://dfrlab.org/2023/06/14/whos-afraid-of-the-sec/.

[14] "Cyber Incident Reporting for Critical Infrastructure Act of 2022," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

[15] Federal Trade Commission Act of 1914, § 5, 15 U.S.C. § 45 (1914).

Cybersecurity as Consumer Protection

The FTC has a mandate to protect consumers and promote competition. Within that ambit, it has the power to bring cases against companies, trade associations, nonprofit organizations, government agencies, and individuals,[16] for a range of practices from phone scams to advertisements for fake COVID-19 cures, thus serving as the enforcer for a dizzyingly swath of the US economy.

The FTC's broad jurisdiction to investigate and curtail "unfair and deceptive acts and practices"[17] (often shortened to UDAP) comes from Section 5a of the Federal Trade Commission Act of 1914 (FTC Act), which states that "unfair or deceptive acts or practices in or affecting commerce… are…declared unlawful."[18] "Deceptive" acts or practices are defined as any "material representation, omission, or practice likely to mislead a consumer otherwise acting reasonably in the circumstances,"[19] and "unfair" acts or practices are those that "cause or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[20]

When it comes to cybersecurity, the FTC can bring actions for deception when a company fails to live up to its claims in privacy policies, marketing materials, or public statements about its security practices or programs (e.g., that it uses "reasonable" or "industry-standard" security practices to protect data). Cyber practices can be unfair when they cause or are likely to cause harm to consumers such as leaking information that could lead to identity theft and when consumers cannot take action to reasonably avoid the harm—typically the case, since most consumers cannot themselves audit a company's security practices. Thus, the FTC has been able to use these twin authorities to bring a variety of cases against companies whose poor cyber practices allowed or could have allowed the theft or leak of consumer information.

The FTC challenges violations of the FTC Act by instituting administrative adjudications. When the commission has reason to believe a violation has occurred or is currently occurring, the commission issues a complaint setting forth the charges. Respondents must either contest these charges in court or settle and enter into a "consent decree." A consent decree does not concede liability, but is a binding agreement for a period, usually twenty years, stipulating specific practices and regulations the defendant must put in place to address the behavior that led to the complaint. For cybersecurity-related failures, consent decrees typically include requirements to establish an adequate data security program with certain mandatory elements. Even when companies choose to challenge the FTC's case, most still result in a consent decree: if a defendant does not settle, the FTC will litigate the case before an administrative law judge, from whom it typically obtains a mandatory injunction requiring defendants to sign a consent decree.

Thus, the FTC's explicit construction as a consumer protection agency fundamentally shapes its approach to cyber enforcement. Its focus is on ensuring companies have adequate (and honestly described) protections to shield consumers from harm caused by improper access to their data, all in order to protect consumers and ensure the fair functioning of the market for consumer goods and services—a market full of products that increasingly implicate the security of consumers' personal data.

[16] Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy,* (New York: Cambridge University Press, 2016), 98.

[17] Federal Trade Commission Act of 1914, § 5, 15 U.S.C. § 45 (1914).

[18] Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(1) (1914).

[19] Federal Trade Commission Act of 1914, 15 U.S.C. § 45(n) (1914).

[20] Federal Trade Commission Act of 1914, 15 U.S.C. § 45(n) (1945).

Methods

This paper is based on a review of the complaints and consent decrees associated with forty-seven cases brought by the FTC for cybersecurity-related UDAP Section 5a violations between 2002 and 2024. The methods focus on three stages: how these cases were selected, how the complaints were analyzed to extract a list of (un)reasonable security practices, and how the consent decrees were analyzed to identify themes and patterns in these FTC-mandated information security programs.

Case Selection

The forty-seven cases in this dataset were identified using tools from the FTC's legal library website and researcher review. First, the research team filtered the FTC's online legal library using built-in tools to a set of cases that were (1) identified as relating to the agency's consumer protection mandate and (2) tagged with "privacy and security." The research team then reviewed this set of 306 cases and selected forty-seven that met two criteria. First, that each case was brought on the basis of, or involved, a cybersecurity failure as instantiated in a vulnerability in or a third-party compromise of an information system. This meant omitting violations that occurred due to insecure disposal, physical theft of sensitive information, or insider threats. Second, that each case was brought based solely on a violation of Section 5a—e.g., an unfair or deceptive act or practice. Thus, the dataset omits cybersecurity-related cases brought on the basis of other laws, such as COPPA or GLBA, and dual violations brought on the basis of violations of both 5a and another law. This second criterion ensures that the analysis of the resulting complaints and consent decrees can speak directly to the strengths and limitations of the FTC's stopgap UDAP authorities versus the specific cybersecurity regulatory authorities granted to it by Congress. An analysis of cases stemming from violations of these specific regulations, and a comparison of those findings with the findings from strictly UDAP cases that make up this dataset, could be a valuable direction for future work.

The texts for the complaints and the consent decrees were obtained using the most recent versions of both documents available via the FTC's online case library. A dataset containing the forty-seven cases, associated metadata, and the links to each complaint and consent decree document is available online, together with text versions of the documents and utility scripts used for data analysis tasks.[21]

As the contents of complaints and consent decrees are referenced frequently in this paper, shorthand names are used throughout. Table 1 in the appendix provides the complete citation for the complaint and consent decree documents corresponding to each shorthand name.

COMPLAINT ANALYSIS

The authors analyzed each complaint document to identify the security failures that formed the basis for the action in order to identify the practices that the FTC understands as having failed to meet the bar for "reasonable" cybersecurity. As such, this component of the analysis omitted three cases[22] in which the FTC alleged deception about a specific security practice—for example, a company that deceptively claimed that a product utilized end-to-end encryption when it did not—since these cases do not implicate a definition of "reasonable" cybersecurity practices. The remaining forty-four complaints all contained the word "reasonable" as applied to cybersecurity practice, further evidence that this subset of the main dataset speaks directly to the FTC's conception of reasonable cyber practice.

The first step in this analysis was the research team's manual review of the data to extract and classify categories of unreasonable practices outlined in each decree. This work was then cross-checked using simple Python scripts that searched all the complaints for relevant keywords related to the practices.

CONSENT DECREE ANALYSIS

Within consent decrees, the researchers analyzed the content and specific provisions of the FTC-mandated security programs to understand how the commission envisions adequate or good cybersecurity practices as well as how they have designed enduring security programs across a variety of organizations.

This analysis was conducted on the full set of forty-seven cases, including the three cases where the defendant made a more specific deceptive claim about their practices. Here again, the bulk of the analytical work was manual researcher review to identify eras and changes between

[21] [GITHUB URL TO COME].

[22] Complaint, BLU Products and Samuel Ohev-Zion, File No. 172-3025, (September 11, 2018); Complaint, 1Health.io/Vitagene, File No. 192-3170, (September 7, 2023); Complaint, Zoom Video Communications Inc., File No. 192-3167, (Feb 1, 2021).

documents. Additionally, researchers used basic natural language processing—embedding the documents as vectors using the bge-small-en model from HuggingFace[23] and then using k-means clustering to group those vectors—to identify clusters of similar consent decrees that were then manually reviewed.

Findings

Overview of the Dataset

The actions within this dataset span from 2002 to 2024. As shown in the graphic below, the first cybersecurity-related cases that the FTC brought were all actions linked to deceptive practices. The first unfairness cases followed a few years later, and within roughly the past decade the agency began bringing actions that accused companies of both unfair and deceptive practices with respect to security.

This dataset contains cases brought against software providers, major retailers, e-commerce platforms, Internet of Things manufacturers, mobile applications, hardware manufacturers, and others. The security failures explored in this paper have contributed to the exposure of consumer names;[24] dates of birth;[25] physical addresses;[26] credit card information including card numbers, expiration dates, and security codes;[27] Social Security numbers (SSNs);[28] bank account and routing numbers;[29] driver’s license numbers;[30] tax returns;[31] medical information including medical history, medication, and examination notes;[32] email addresses;[33] video recordings of homes;[34] and communications with loved ones.[35]

[23] Shitao Xiao et al., “C-Pack: Packaged Resources To Advance General Chinese Embedding,” *arXiv*, last updated May 12 2024, https://doi.org/10.48550/arXiv.2309.07597.

[24] See Appendix 1: James V. Grago, Jr. (ClixSense) Complaint.

[25] See Appendix 1: ASUSTeK Complaint.

[26] See Appendix 1: James V. Grago, Jr. (ClixSense) Complaint.

[27] See Appendix 1: DSW Complaint.

[28] See Appendix 1: Reed Elsevier Complaint.

[29] See Appendix 1: InfoTrax Complaint.

[30] See Appendix 1: Uber Complaint.

[31] See Appendix 1: ASUSTeK Complaint.

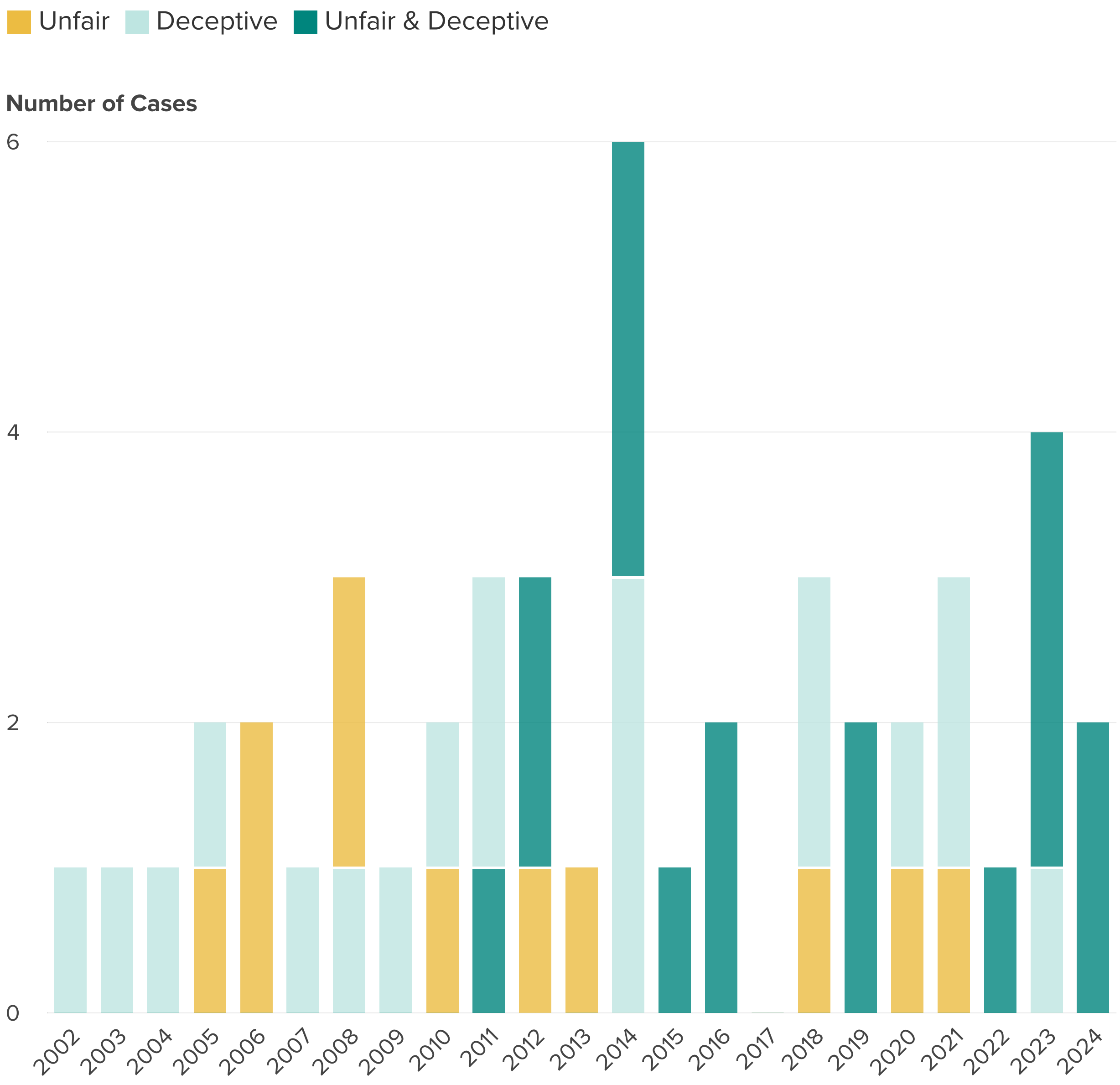
[32] See Appendix 1: Blackbaud Complaint.

[33] See Appendix 1: Genelink Complaint.

[34] See Appendix 1: Zoom Complaint.

[35] See Appendix 1: Blackbaud Complaint.

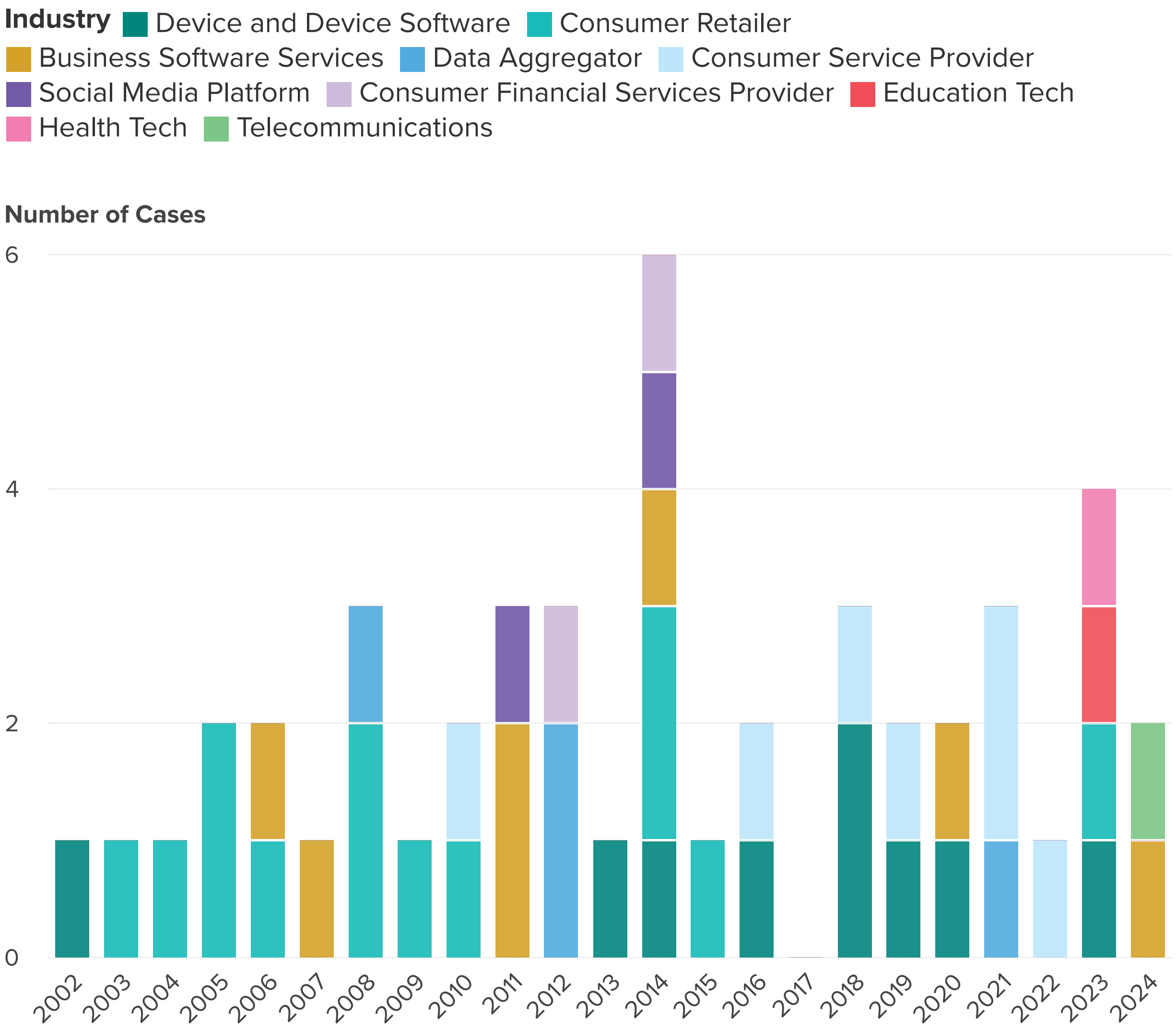
Figure 1: Unfair Versus Deceptive Cyber Cases Over Time.



NOTE: The number of cases in the dataset brought on the basis of unfair cybersecurity practices, deceptive cybersecurity practices, or both unfair and deceptive cybersecurity practices, per year.

SOURCES: FTC complaints.

Figure 2: FTC UDAP Cyber Cases by Sector



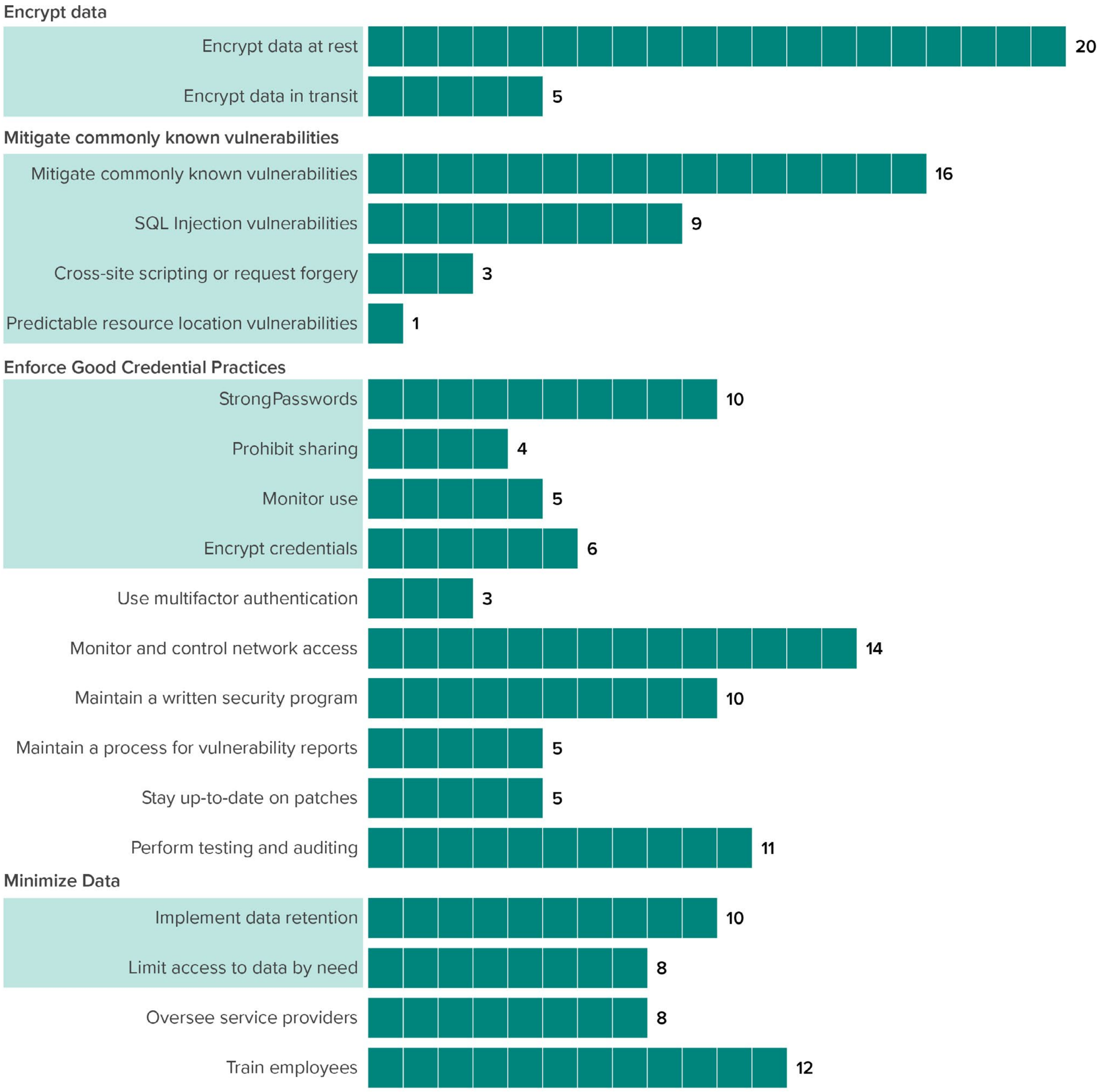
NOTE: The number of cases brought in the dataset by the primary sector or function of the defendant company.
SOURCES: FTC complaints.

Reasonable Cybersecurity Practices: The Complaints

Complaints filed as a part of FTC actions outline the alleged misconduct of a defendant, providing the clearest understanding of the types of practices that the FTC considers unfair or deceptive when it comes to processing and protecting consumer data. Each complaint lists ways in which the defendant’s practices—individually and collectively—failed to provide “reasonable or appropriate security” for the consumer information they collected. Thus, through their evolving adjudication of Section 5a cases, the FTC has expanded and evolved a de facto list of inadequate data security practices.

While these security failures differ from case to case and evolved over time to include practices relating to newer technologies (e.g., the failure to securely store cloud bucket credentials), certain security failures have persisted throughout the two decades of FTC complaints. Distilling the shortcomings outlined in these complaints provides both a window into the FTC’s conception of reasonable baseline security practices for companies that interact with consumer data and a repository of information about security failures that have caused tangible consumer harm.

Figure 3: Cybersecurity Practices in FTC Complaints



NOTE: The number of complaints that name the listed practice as one of the practices that, taken together, failed to provide reasonable security.
SOURCES: FTC complaints.

1. Encrypt Data

Encryption—the practice of cryptographically transforming data so that it is unreadable to those without the proper "key" to decrypt it—has been a fundamental building block of information security since at least the 1970s.[36]

ENCRYPT DATA AT REST

Encrypting data at rest means applying encryption to data that is statically stored in databases or other locations on an information system. The dataset reviewed in this report contained twenty complaints[37] in which the FTC identified, as an unreasonable security practice, a company storing consumer information at rest in an unencrypted format. These cases span from 2005 to 2024 and include cases in which defendants were storing cleartext (i.e., unencrypted) data in on-premise and cloud databases alike.[38]

ENCRYPT DATA IN TRANSIT

Encrypting data in transit refers to encrypting data as it moves around an information system, such as when it is transmitted over the internet. In five cases,[39] the FTC identified the failure to encrypt consumer data in transit as an unreasonable or inadequate security practice. These cases include instances where companies failed to encrypt user data as it was transmitted over the internet[40] and where companies sent unencrypted information within their corporate network.[41]

2. Mitigate Commonly Known Vulnerabilities

Vulnerabilities in software make it possible for an attacker to take undesired actions such as escalating their access or accessing resources that are supposed to be restricted. While some vulnerabilities are sophisticated and hard to detect ahead of time, many arise from commonly known weaknesses.[42] In seventeen complaints,[43] the FTC identified failures to mitigate "commonly known" (or "well-known") or "reasonably foreseeable" vulnerabilities and attacks in their websites or products as an unreasonable security practice. These included failure to:

- Mitigate Standard Query Language (SQL) injection vulnerabilities, with nine cases from across the dataset—the most recent in 2023[44]
- Prevent cross-site scripting attacks[45] or cross-site request forgeries[46]
- Prevent predictable resource location vulnerabilities[47]

The FTC's language around these vulnerabilities typically emphasized that they were commonly known vulnerabilities—showing that they had been the subject of warnings from security experts or had been featured in previous publicly reported security incidents. These criteria are discussed in further detail at the end of this section.

3. Enforce Good Credential Practices

Enforcing good credential-management practices—both for customer and employee credentials—is a long-running theme within this dataset, appearing in complaints

[36] "History of Encryption," Thales Group, last updated June 10, 2023, https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption.

[37] See Appendix 1: DSW Complaint; Guidance Software Complaint; Life is Good Complaint; TJX Complaint; Genica Complaint; LifeLock Complaint; Ceridian Complaint; Upromise Complaint; TRENDnet Complaint; Wyndham Complaint; Uber Complaint; James V. Grago, Jr. (ClixSense) Complaint; D-Link Complaint; InfoTrax Complaint; Support King Complaint; SkyMed Complaint; Ring Complaint; Residual Pumpkin (CafePress) Complaint; Chegg Complaint; Global Tel*Link Complaint.

[38] See Appendix 1: InfoTrax Complaint.

[39] See Appendix 1: BJ's Complaint; TJX Complaint; LifeLock Complaint; Upromise Complaint; Compete Complaint.

[40] See Appendix 1: Compete Complaint.

[41] See Appendix 1: LifeLock Complaint.

[42] "Common Weakness Enumerations," MITRE, last updated May 13, 2024, https://cwe.mitre.org/.

[43] See Appendix 1: Guess Complaint; MTS (Tower Records) Complaint; Petco Complaint, Card Systems Solutions Complaint; Guidance Software Complaint; Life is Good Complaint; Reed Elsevier Complaint; Genica Complaint; Ceridian Complaint; ASUSTek Complaint; James V. Grago, Jr. (ClixSense) Complaint; LifeLock Complaint; Lookout Services Complaint; D-Link Complaint.

[44] See Appendix 1: Guess Complaint; Petco Complaint; Card Systems Solutions Complaint; Guidance Software Complaint; Life is Good Complaint. Genica Complaint; LifeLock Complaint; Ceridian Complaint; Residual Pumpkin (CafePress) Complaint.

[45] See Appendix 1: Reed Elsevier Complaint; ASUSTeK Complaint; Residual Pumpkin (CafePress) Complaint.

[46] See Appendix 1: ASUSTeK Complaint; Residual Pumpkin (CafePress) Complaint.

[47] See Appendix 1: Lookout Services Complaint.

associated with cases from 2006 to cases from 2022. Since credentials are the "keys to the kingdom" that allow access to sensitive user information and organizational resources, protecting credentials and making it difficult for attackers to obtain or guess them is a core principle in information security.

STRONG PASSWORDS AND HARD-TO-GUESS CREDENTIALS

The FTC has identified the use of weak or easy-to-guess passwords or credentials in ten cases[48] in this dataset as a bad practice both for employee and user credentials. Specifically, the FTC identified the failure to:

- Make administrative passwords difficult to guess[49] or to require network administrators to use strong passwords[50]
- "Establish or enforce rules sufficient to make user credentials hard to guess"[51]
- "Require employees, vendors, and others with access to personal information to use hard-to-guess passwords"[52]

PROHIBIT SHARING OF CREDENTIALS

In four of the cases[53] contained in this dataset, the FTC has identified as an unreasonable practice that a company allowed users,[54] employees,[55] or third parties[56] to share credentials. This also included cases where companies allowed employees to reuse passwords to access multiple servers and services,[57] or "permit[ed] all programs and engineers to use a single AWS access key that provided full administrative privileges over all data in the Amazon S3 Datastore."[58]

MONITOR USE OF CREDENTIALS

Monitoring the use of credentials to identify suspicious patterns can help prevent attackers from obtaining and abusing legitimate credentials. Five complaints[59] in the dataset referenced defendants' failure to monitor the use of credentials, including lacking a way to "monitor unsuccessful log-in attempts,"[60] or "suspend user credentials after a certain number of unsuccessful log-in attempts."[61]

ENCRYPT CREDENTIALS

Storing or transmitting credentials without encryption can allow attackers to more easily steal the credentials from devices or as they are sent over the network. The FTC has faulted companies for:

- Transmitting user credentials in cleartext[62]
- Allowing users to "store their user credentials in a vulnerable format in [unencrypted] cookies"[63]
- Using "outdated and unsecure cryptographic hash functions to protect users' passwords"[64]

The FTC has also found it unreasonable for companies to lack policies and controls that would prevent employees from storing unencrypted credentials on their machines or systems, faulting companies for failure to "prohibit storage of administrative passwords in plain text"[65] or "prevent the

[48] See Appendix 1: Reed Elsevier Complaint; LifeLock Complaint; Wyndham Complaint; Residual Pumpkin (CafePress) Complaint.

[49] See Appendix 1: Twitter Complaint.

[50] See Appendix 1: Card Systems Solutions Complaint; TJX Complaint; Twitter Complaint; ASUSTeK Complaint; Drizly Complaint; Blackbaud Complaint.

[51] See Appendix 1: Reed Elsevier. Complaint.

[52] See Appendix 1: LifeLock Complaint.

[53] See Appendix 1: Reed Elsevier Complaint; Ashley Madison Complaint; Uber Complaint; James V. Grago, Jr. (ClixSense) Complaint.

[54] See Appendix 1: Reed Elsevier Complaint.

[55] See Appendix 1: Ashley Madison Complaint.

[56] See Appendix 1: James V. Grago, Jr. (ClixSense) Complaint.

[57] See Appendix 1: Ashley Madison Complaint.

[58] See Appendix 1: Uber Complaint.

[59] See Appendix 1: Reed Elsevier Complaint; LifeLock Complaint; Lookout Services Complaint; Twitter Complaint; Ashley Madison Complaint.

[60] See Appendix 1: Ashley Madison Complaint.

[61] See Appendix 1: Reed Elsevier Complaint.

[62] See Appendix 1: Guidance Software Complaint; Lookout Services Complaint; TRENDnet Complaint; James V. Grago, Jr. (ClixSense) Complaint.

[63] See Appendix 1: Reed Elsevier Complaint.

[64] See Appendix 1: Chegg Complaint.

[65] See Appendix 1: Twitter Complaint.

retention of passwords and encryption keys in clear text files."[66]

[DEPRECATED BEST PRACTICE] REQUIRE PERIODIC CHANGING OF CREDENTIALS

Changing user credentials is one area where the FTC has evolved its approach over time. Between 2008 and 2011, four complaints faulted defendants for failing to enforce or require the periodic change of user credentials or administrative passwords. However, the FTC has revised its thinking on this issue—in 2016 it published a blogpost suggesting that organizations "rethink mandatory password changes," citing recent findings in the information security field suggesting that this practice did not actually improve security.[67] And, no complaints after 2016 list a failure to require periodic changing of credentials as an unreasonable practice. This deprecated practice shows that the FTC has evolved the practices it cites as a threat to cybersecurity based on broader consensus within the information security field.

4. Use Multifactor Authentication

Multifactor authentication is a way of enhancing the security of username-and-password requirements for authentication by requiring a "third factor" such as a mobile device or security key in possession of the user. Multifactor authentication can stop attacks such as those in which threat actors use leaked user credentials to log into information systems, since the attackers will lack access to the third factor needed to log in. Three of the complaints[68]—all of them recent, from 2022 to 2024—cite companies' failure to use multifactor authentication as an unreasonable practice.

5. Monitor and Control Network Access

Attackers who can successfully infiltrate an organization's network can potentially access sensitive data and resources or deploy malware such as ransomware. In fourteen of the cases[69] included in this dataset, the FTC faulted defendants for failing to implement adequate practices for monitoring and controlling network access. These include failures to limit access between a defendant's network and the internet, including by:

- Using firewalls between the internet and a corporate network[70] and limit access between computers within the corporate network[71]
- Limiting access through wireless access points to networks[72]
- Using "reasonable" or "sufficient" measures to detect or investigate unauthorized network access, such as intrusion detection systems or monitoring and reviewing logs[73]
- Monitoring their networks and systems for attempts to transfer or exfiltrate data outside of network boundaries[74]
- Restricting inbound connections to known IP addresses[75] (a more novel safeguard, from only one recent case)

6. Maintain a Written Security Program

A written security program can help organizations lay out a plan for how they will implement necessary controls and oversight within their network, as well as how they will respond to security incidents or other events. Ten of the FTC complaints[76] invoke either the nonexistence or the

[66] See Appendix 1: Ashley Madison Complaint.

[67] Lorrie Cranor, "Time to Rethink Mandatory Password Changes," *Federal Trade Commission (Office of Technology Blog)*, March 2, 2016, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2016/03/time-rethink-mandatory-password-changes.

[68] See Appendix 1: Drizly Complaint; Chegg Complaint; Blackbaud Complaint.

[69] See Appendix 1: BJ's Complaint; TJX Complaint; Card Complaint; DSW Complaint; Genica Complaint, Guidance Software Complaint; Life is Good Complaint; Dave & Busters Complaint; Wyndham Complaint; James V. Grago, Jr. (Clixsense) Complaint; SkyMed Complaint; Chegg Complaint; Global Tel*Link Complaint; Blackbaud Complaint.

[70] See Appendix 1: TJX Complaint; Dave & Busters Complaint; Wyndham Complaint.

[71] See Appendix 1: Card Complaint; DSW Complaint; Genica Complaint; Dave & Busters Complaint; James V. Grago, Jr. (ClixSense) Complaint.

[72] See Appendix 1: BJ's Complaint; DSW Complaint; TJX Complaint; Dave & Busters Complaint.

[73] See Appendix 1: Genica Complaint; LifeLock Complaint; Dave & Busters Complaint; Lookout Services Complaint; EPN Checknet complaint; Wyndham Complaint.

[74] See Appendix 1: SkyMed Complaint; EPN Checknet Complaint; Chegg Complaint; Blackbaud Complaint.

[75] See Appendix 1: Drizly Complaint.

[76] See Appendix 1: EPN CheckNet Complaint; Ashley Madison Complaint; Uber Complaint; Tapplock Complaint; SkyMed Complaint; Drizly Complaint, Chegg Complaint; SkyMed Complaint; Chegg Complaint.

inadequacy of a defendant's written information security program as an unreasonable practice. The FTC mentions components of such a plan including:

- An incident response plan[77]
- "Standards, policies, procedures, or practices" for data security[78]
- "Standards, policies, procedures or practices" for third-party software[79]

7. Maintain a Process for Accepting and Addressing Vulnerability Reports

Users or independent security researchers can detect vulnerabilities in a company's product or network before the company does; in these cases, it is beneficial for the company to have standard practices by which these users and researchers can report vulnerabilities for resolution so their reports are not lost or overlooked. In five of the complaints in this dataset,[80] the FTC described as unreasonable that the defendant failed to have a process for monitoring, receiving, and addressing external security vulnerability reports. Various complaints emphasized that this lack of a process "delay[s] the opportunity to correct discovered vulnerabilities or respond to reported incidents"[81] or highlighted the "existence of free tools to conduct such monitoring."[82]

8. Stay Up to Date with Patches

Attackers can exploit known vulnerabilities in unpatched software to gain a foothold into the network. Timely application of critical patches for software used within a company's network can help protect companies from this threat. Five complaints[83] in the dataset mentioned companies' failure to patch the software they used in a timely manner as an unreasonable practice, including, specifically:

- Failure to patch servers running on their network[84]
- Failure to patch security tools such as antivirus software[85]
- Using versions of software that no longer received patches[86]
- Failure to "implement patch management policies and procedures to ensure the timely remediation of critical security vulnerabilities and [use of] obsolete versions of database and web server software that no longer received patches"[87]

9. Perform Testing and Auditing

Proactive testing and auditing of software products, websites, and corporate networks can help an organization proactively identify points of weakness or vulnerability, which could be targeted by malicious actors. The FTC cited the lack of proactive testing and auditing (such as penetration testing) in eleven of its complaints,[88] including:

- Failure to penetration test networks[89]
- Failure to penetration test software or applications[90]
- Failure to penetration test hardware devices[91]
- Failure to test software "such as by inputting invalid, unanticipated, or random data to the software"[92]
- Failure to perform code review of software systems[93]

[77] See Appendix 1: EPN CheckNet Complaint.

[78] See Appendix 1: Tapplock Complaint; SkyMed Complaint; Drizly Complaint; Chegg Complaint; SkyMed Complaint; Chegg Complaint.

[79] See Appendix 1: Lenovo Complaint.

[80] See Appendix 1: HTC America Complaint; Fandango Complaint; TRENDnet Complaint; ASUSTeK Complaint; Residual Pumpkin (CafePress) Complaint.

[81] See Appendix 1: HTC America Complaint; TRENDnet Complaint; ASUSTeK Complaint.

[82] See Appendix 1: TRENDnet Complaint.

[83] See Appendix 1: TJX Complaint; Wyndham Complaint; Residual Pumpkin (CafePress) Complaint; Blackbaud Complaint; LifeLock Complaint.

[84] See Appendix 1: Wyndham Complaint; Residual Pumpkin (CafePress) Complaint; LifeLock Complaint.

[85] See Appendix 1: TJX Complaint.

[86] See Appendix 1: Wyndham Complaint; Residual Pumpkin (CafePress) Complaint.

[87] See Appendix 1: Residual Pumpkin (CafePress) Complaint.

[88] See Appendix 1: Upromise Complaint; HTC America Complaint; Fandango Complaint; Credit Karma Complaint; TRENDnet Complaint; ASUSTeK Complaint; InfoTrax Complaint; Tapplock Complaint; SkyMed Complaint; Drizly Complaint; Blackbaud Complaint.

[89] See Appendix 1: InfoTrax Complaint; SkyMed Complaint; Drizly Complaint.

[90] See Appendix 1: Fandango Complaint; Credit Karma Complaint; TRENDnet Complaint; ASUSTeK Complaint.

[91] See Appendix 1: HTC America Complaint.

[92] See Appendix 1: TRENDnet Complaint.

[93] See Appendix 1: TRENDnet Complaint; ASUSTeK Complaint; InfoTrax Complaint.

- Failure to "test the [software] before distributing it to consumers or monitor the [software]'s operation thereafter to verify that the information it collected was consistent with respondent's policies"[94]
- Failure to "test, audit, assess, or review its products' or applications' security features; and conduct regular risk assessments, vulnerability scans, and penetration testing of its networks and databases[95]

10. Minimize Data Retention and Access

IMPLEMENT DATA RETENTION

One way to protect consumers is to delete their data when it is no longer necessary for a business purpose—even if a hack were to occur, hackers cannot steal data that is not there. In this dataset, the FTC has faulted ten companies[96] for retaining unnecessary consumer information, citing failures including:

- Storage of consumer information "indefinitely" on their networks "without a business need"[97]
- Lack of "appropriate data retention schedules and deletion practices"[98]
- Lack of "policy, process, or procedure" for "inventorying and deleting" consumer and employee information that was no longer needed[99]

LIMIT ACCESS TO DATA BY NEED

Another way for companies to protect consumer information is to make sure that employees access to consumer information is limited to what is required to do their job: if every user has access to every resource, then if any one of them is compromised, the company's trove of data is at risk. In the dataset, the FTC faulted eight companies[100] for failing to implement access controls for consumer information—that is, failing to ensure access to sensitive data is limited to employees or individuals with a direct business need. This includes restricting their access to consumers' sensitive information based on their job function.[101]

Purpose-limited access is not only applicable to sensitive consumer information, but also applies to employees' access to security controls or security-relevant resources like source code. FTC complaints have faulted companies for continuing to allow employees to have access to administrative controls[102] or source code[103] after they no longer needed such access.

11. Oversee Service Providers

In addition to the primary defendants in FTC cases, third-party service providers often also have access to sensitive consumer data. These service providers include third-party cloud service providers as well as companies that "receive, process, or maintain"[104] consumer information on behalf of the primary defendant. In eight complaints contained in this dataset, the commission has suggested that defendants must oversee their service providers.[105] Some cases[106] suggested that companies should require their service providers, by contract, to adopt specific practices, including:

- To implement "simple, low-cost, and readily available defenses to protect consumers' personal information"[107]
- To provide employees with "secure development training or other data security training appropriate to their job duties"[108]

[94] See Appendix 1: Upromise Complaint.

[95] See Appendix 1: Drizly Complaint; Blackbaud Complaint.

[96] See Appendix 1: BJ's Complaint; DSW Complaint; Life is Good Complaint; Ceridian Complaint; Residual Pumpkin (CafePress) Complaint; InfoTrax Complaint; SkyMed Complaint; Drizly Complaint; Chegg Complaint; Blackbaud Complaint.

[97] See Appendix 1: Residual Pumpkin (CafePress) Complaint.

[98] See Appendix 1: Blackbaud Complaint.

[99] See Appendix 1: Chegg Complaint.

[100] See Appendix 1: LifeLock Complaint; Twitter Complaint; Ashley Madison Complaint; Uber Complaint; InfoTrax Complaint; Support King Complaint; Drizly Complaint; Ring Complaint.

[101] See Appendix 1: Ashley Madison Complaint; Ring Complaint.

[102] See Appendix 1: Twitter Complaint.

[103] See Appendix 1: Drizly Complaint.

[104] See Appendix 1: Global Tel*Link Complaint.

[105] See Appendix 1: Upromise Complaint; Genelink Complaint; Credit Karma Complaint; GMR Transcription Services Complaint; Ashley Madison Complaint; Lenovo Complaint; Support King Complaint; Global Tel*Link Complaint.

[106] See Appendix 1: Tel*Link Complaint; Ashely Madison Complaint; Support King Complaint.

[107] See Appendix 1: Global Tel*Link Complaint.

[108] See Appendix 1: Global Tel*Link Complaint.

12. Train Employees and Personnel

Training employees and personnel in security practices can help them understand and implement proper security practices in their day-to-day work, from avoiding clicking on phishing links to properly configuring software systems that process consumer data. The failure to adequately train personnel was an unreasonable practice mentioned in twelve of the complaints in this dataset.[109] These instances include:

- Failure to provide employees with "data security training" or to train personnel "to perform their data security related duties and responsibilities"[110]
- Failure to provide employees with "adequate guidance" regarding information security[111]
- Failure to provide adequate training to "engineering staff,"[112] or to employees responsible for "testing third-party software"[113] or "designing, testing, overseeing, and approving software specifications and requirements "[114]

Analysis: How the FTC Constructs Reasonableness

Analyzing the above complaints reveals a few ways in which the FTC constructs and supports its argument that a company's practices fail to provide reasonable cybersecurity for its customers.

1. Foreseeability: Expert Warnings, Industry Practice, and Prior Attacks

To justify why a practice should be considered unreasonable, the FTC explicitly refers to widely available information about a vulnerability or practice as evidence that the defendant should have known that they needed to address (or avoid) the failure.

One such reason is that security experts have already issued public warnings about a practice or attack. For example, in one complaint, the FTC wrote, "security professionals have issued public warnings about the security risk presented by weak user ID and password structures since the late 1990s,"[115] and at least five other complaints include references to "security experts" or "security professionals" when arguing that a company should have reasonably known that its practice was flawed.

The FTC also references broader industry consensus, such as citing causes of cybersecurity weaknesses "commonly known in the information technology industry."[116]

Additionally, in some cases, the FTC relies on publicly disclosed incidents attributable to similar flaws or practices to make the case that a company should have known that a particular practice was unreasonably risky. In its 2022 case against Drizly, the FTC stated, "numerous publicly reported security incidents since 2013 have highlighted the dangers of storing passwords and other access keys in GitHub repositories,"[117] using real-world patterns of cyber incidents to support its claim that the company's practices clearly failed to provide a reasonable measure of security.

These approaches are not mutually exclusive—for example, addressing failures to mitigate commonly known web application vulnerabilities, the FTC in a single complaint said that "the risk of such web application attacks is well known in the information technology industry [...] security experts have been warning the industry about these vulnerabilities since

[109] See Appendix 1: MTS (Tower Records) Complaint; Compete Complaint; Upromise Complaint; HTC America Complaint; TRENDnet Complaint; Ashely Madison Complaint; Lenovo Complaint; Uber Complaint; Tapplock Complaint; SkyMed Complaint; Ring Complaint; Chegg Complaint.

[110] See Appendix 1: Ashely Madison Complaint.

[111] See Appendix 1: Chegg Complaint, SkyMed Complaint.

[112] See Appendix 1: HTC America Complaint.

[113] See Appendix 1: Lenovo Complaint.

[114] See Appendix 1: Tapplock Complaint.

[115] See Appendix 1: Reed Elsevier Complaint.

[116] See Appendix 1: Ceridian Complaint.

[117] See Appendix 1: Drizly Complaint.

at least 1997; [...] and in 2000 the industry began receiving reports of successful attacks on web applications."[118]

2. Availability and Cost of Mitigations

The FTC also factors into its arguments the existence of "readily available" and "free or low-cost"[119] tools that would have mitigated the causes of failure. For example, in one complaint, the FTC stated that the defendant failed to encrypt credentials "despite the existence of free software, publicly available since 2008, that would have enabled respondent to secure such stored credentials."[120] This statement emphasizes that software mitigations were publicly available, that they had been available for a long time, and that they were available at no cost, presumably to make even clearer the unreasonable nature of the defendant's failure to adopt such safeguards.

3. Prior FTC Actions

Aside from providing specific examples of industry standard security practices in their complaints, the FTC also points to previous cases to reinforce the point that the defendant should have known that its security behavior was unfair or deceptive.

For example, in a 2022 complaint, the FTC highlighted how "the Commission's 2018 Complaint against Uber Technologies, Inc. specifically publicized and described credential reuse, lack of multifactor authentication, and insecure AWS credentials exposed through GitHub repository code as failures contributing to the breach and exposure of consumers' personal information,"[121] further bolstering the commission's argument that the defendant should have known that these practices were unreasonable and insufficient to provide adequate security.

Comprehensive Security Programs, Per the FTC: Consent Decrees

Consent decrees are legally binding agreements between a defendant and the FTC that stipulate the actions the defendant must take to remediate some legal breach or violation. Most data security-related decrees begin by listing prohibitions on certain activities that led to the original complaint. Then, the order lists the mandated comprehensive security program that the defendant must implement. From there, defendants are required to obtain initial and biennial data security assessments for a stipulated amount of time (typically twenty years). The next part of the decree requires the defendant to disclose all necessary information to the security assessor and to submit an annual certification to the FTC that the defendant has implemented the requirements listed in the consent decree. The final part of the consent decrees includes a reporting and compliance provision, such as recordkeeping requirements. The subsequent analysis focuses specifically on the security program mandated by the consent decrees. These security programs provide a window into how the FTC thinks about adequate cybersecurity practices for companies, and, without a clear cybersecurity law in place, other companies (beyond those required to) have looked to the FTC's consent decrees to guide their cybersecurity practices.

The below visualization highlights the changes across the security programs mandated in FTC consent decrees throughout the history of the dataset.

What Makes a Comprehensive Information Security Program?

1. Identify Risks, Implement Safeguards

Microsoft (2002)

In 2002, the FTC entered into the dataset's first consent decree, settling with Microsoft Corporation on charges that the company had falsely represented their data and security practices. Ordering Microsoft to establish and maintain

[118] See Appendix 1: Guess Complaint.

[119] See Appendix 1: Ceridian Complaint.

[120] See Appendix 1: TRENDnet Complaint.

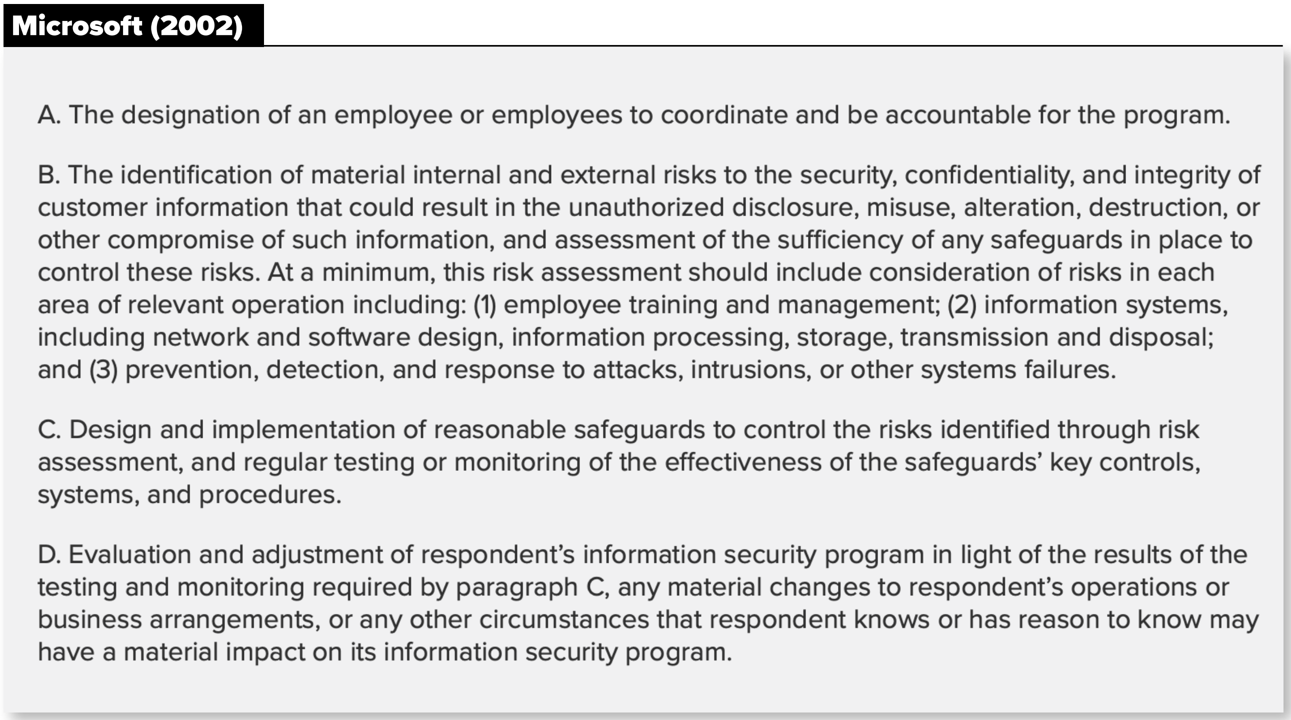
[121] See Appendix 1: Drizly Complaint.

"a comprehensive security program," this consent decree would define the language that persisted throughout decades of consent decrees to follow. The security program was to be established in writing, designed to protect the "security, confidentiality, and integrity" of consumer information, and to include "administrative, technical and physical safeguards" appropriate for Microsoft's size, complexity, the nature of their activities, and the sensitivity of the consumer information they collected. It also included a few specific additional requirements:

- Designation of an employee to lead the information security program
- Identification of risks to the confidentiality, security, and integrity of customer information that could result in its unauthorized use or disclosure
- Assessment of existing safeguards for mitigating such risks, including, specifically:
  - "employee training and management;"
  - "information systems, including network and software design, information processing, storage, transmission, and disposal;" and
  - "prevention, detection, and response to attacks, intrusions, or other systems failures."[122]
- Design and implementation of safeguards to control the identified risks
- Regular testing or monitoring of these safeguards
- Ongoing evaluation, monitoring, and updating of the information security program itself, according to the identified risks and the results of the testing of the safeguards[123]

This is, broadly, a risk-based approach. Rather than requiring Microsoft to adopt specific safeguards or practices, the FTC placed upon them the impetus to identify risks to customer information and design appropriate (and documented) safeguards. This risk-based approach was to become an enduring feature of the cybersecurity consent decrees within this dataset.

Figure 4: Microsoft Consent Decree



Microsoft (2002)

A. The designation of an employee or employees to coordinate and be accountable for the program.

B. The identification of material internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation including: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. Evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by paragraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on its information security program.

[122] See Appendix 1: Microsoft Order.

[123] See Appendix 1: Microsoft Order.

2. Oversee Your Service Providers

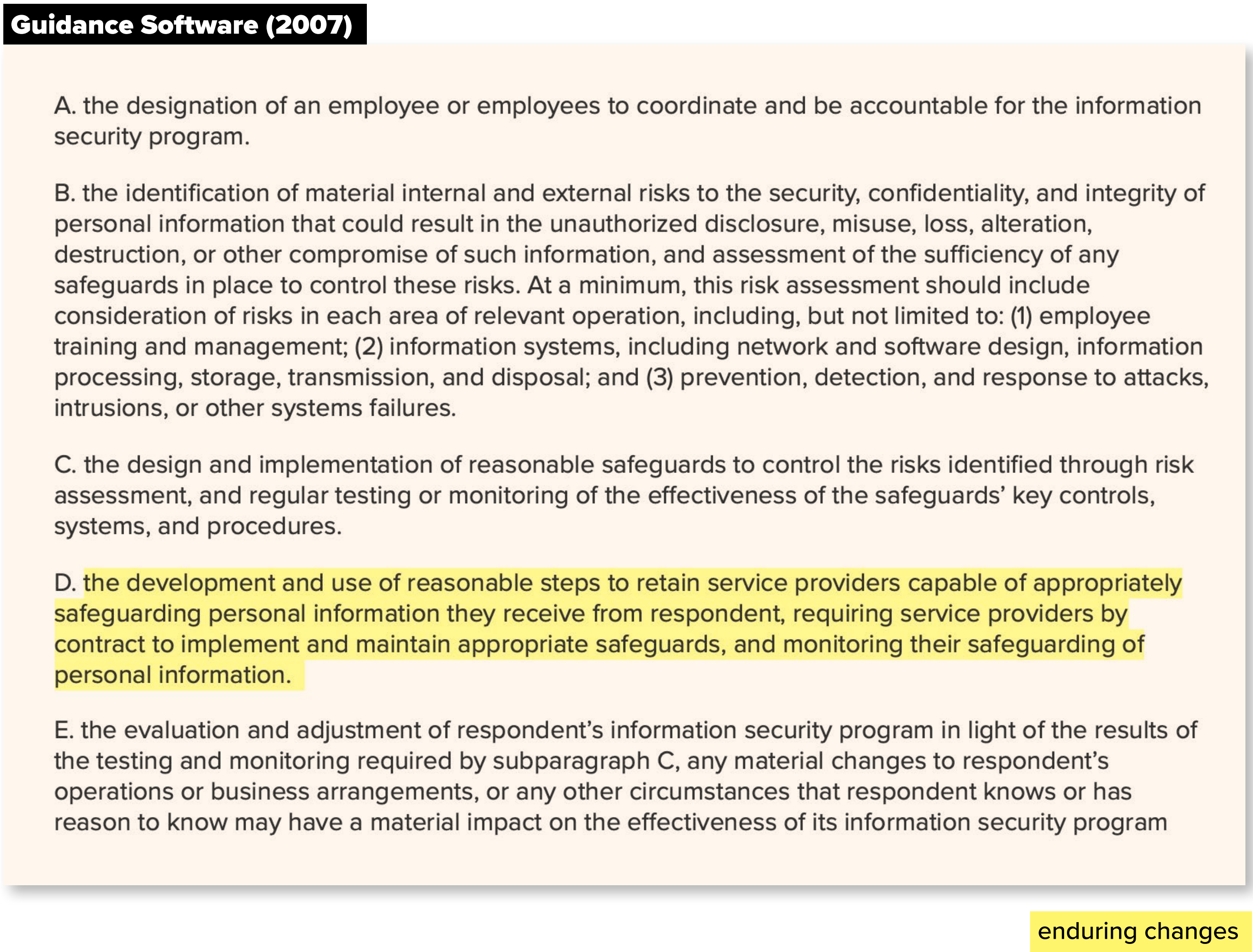
Guidance Software (2007)

In 2007, the FTC settled with Guidance Software, a vendor of software and materials, services, and training for customers to investigate and respond to computer breaches and security incidents. Included in the Guidance Software consent decree was a new requirement that would become ingrained in consent decree language going forward:

- Developing and implementing "reasonable steps" to work only with service providers "capable of appropriately safeguarding personal information;"
- Requiring services providers, by contract, to implement and maintain "appropriate safeguards;" and
- Monitoring service providers' protection of personal information.[124]

At first glance, these new provisions seem surprising. According to what is recorded in the complaint, Guidance Software was not harmed by a service provider; instead, it *was* the service provider, and its website's vulnerability to SQL injection harmed the companies that were its customers. Thus, this change seems to suggest that the FTC may intentionally use consent decrees to set broader standards, beyond responding to the narrow circumstances of a single instance of failure, based on its knowledge of the range of practices that could harm security.[125] (This idea was partially at issue, in fact, in a later legal challenge to the FTC's decrees.)

Figure 5: Guidance Software Consent Decree



Guidance Software (2007)

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondent, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information.

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program

enduring changes

[124] See Appendix 1: Guidance Software Order.

[125] See Appendix 1: Guidance Software Order.

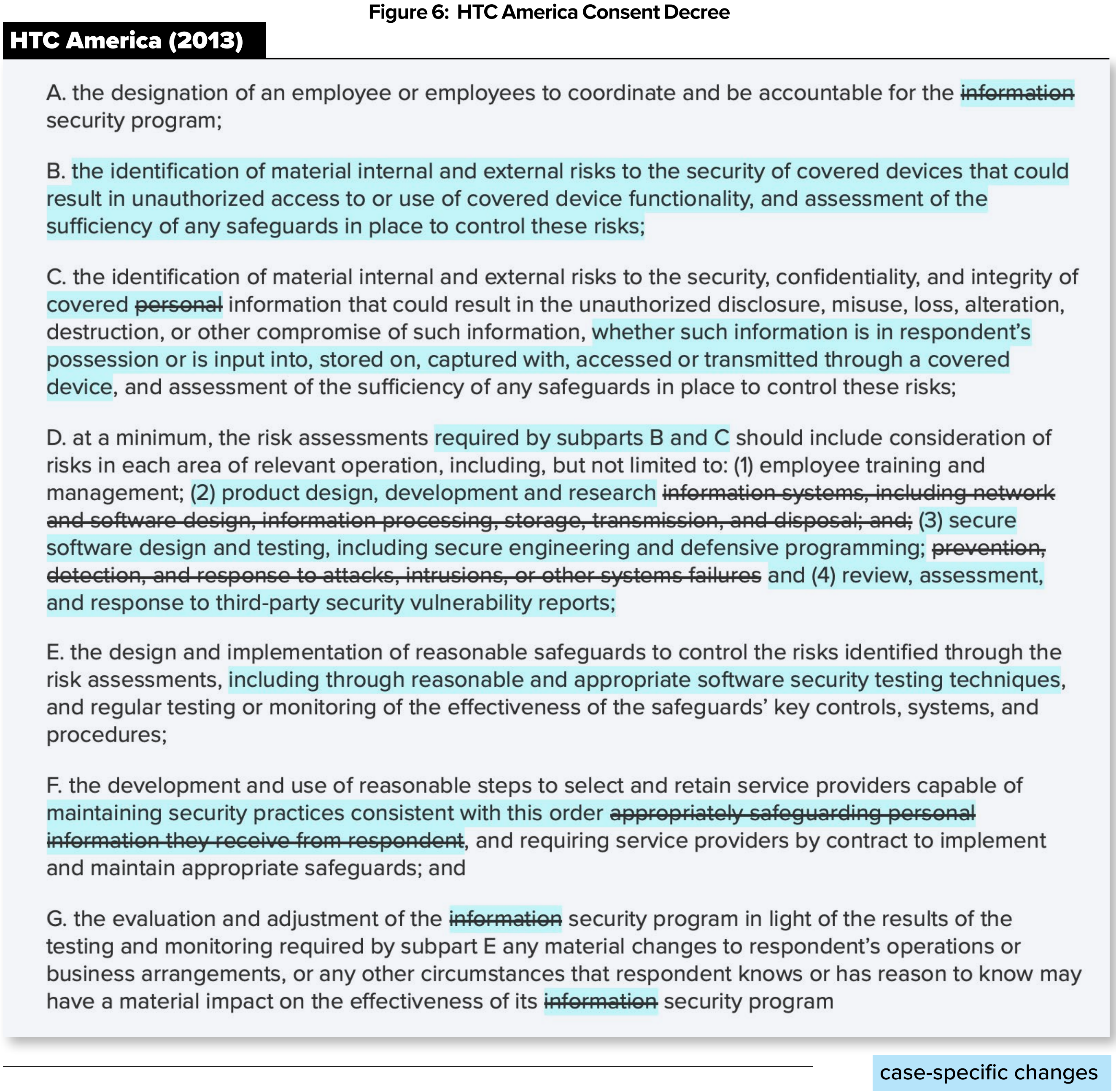
3. Insecure Devices

HTC America (2013), TRENDnet (2014)

HTC America was one of the first cases in the dataset that addressed insecure devices rather than insecure corporate networks. Therefore, the consent decree had some unique features. For example, it made reference to “material internal and external risks to the security of covered devices that could result in unauthorized access to or use of covered device functionality,” rather than risks to consumer information. It also required:

- That the mandatory security program include an assessment of risks and the adequacy of safeguards related to:
  - “product design, development and research;”
  - “secure software design and testing, including secure engineering and defensive programming;” and
  - “review, assessment, and response to third-party security vulnerability reports.”
- That implemented safeguards be evaluated “through reasonable and appropriate software security testing techniques”[126]

Figure 6: HTC America Consent Decree



HTC America (2013)

A. the designation of an employee or employees to coordinate and be accountable for the ~~information~~ security program;

B. the identification of material internal and external risks to the security of covered devices that could result in unauthorized access to or use of covered device functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

C. the identification of material internal and external risks to the security, confidentiality, and integrity of covered ~~personal~~ information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent’s possession or is input into, stored on, captured with, accessed or transmitted through a covered device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. at a minimum, the risk assessments required by subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development and research ~~information systems, including network and software design, information processing, storage, transmission, and disposal; and;~~ (3) secure software design and testing, including secure engineering and defensive programming; ~~prevention, detection, and response to attacks, intrusions, or other systems failures~~ and (4) review, assessment, and response to third-party security vulnerability reports;

E. the design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including through reasonable and appropriate software security testing techniques, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

F. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order ~~appropriately safeguarding personal information they receive from respondent~~, and requiring service providers by contract to implement and maintain appropriate safeguards; and

G. the evaluation and adjustment of the ~~information~~ security program in light of the results of the testing and monitoring required by subpart E any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its ~~information~~ security program

case-specific changes

[126] See Appendix 1: HTC America Order.

These changes reflected the FTC's adaptation of its core security program requirements to apply to an entity that sold devices and software to consumers, rather than operating software systems that processed consumer data. The consent decrees for ASUSTeK and TRENDnet—two computing device sellers—contained similar requirements, but added a more specific requirement that "appropriate software security testing techniques" should include practices such as "(1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to covered information is restricted consistent with a user's security settings."

4. Insecure Applications

Fandango (2014), Credit Karma (2014))

On August 21, 2014, the FTC settled charges with two companies—Fandango and Credit Karma—after their security failures left consumer information vulnerable despite assurances that their mobile apps were secure.[127] The consent decrees for these cases built upon the precedent set in the insecure device cases, adding similar requirements, including to assess risks related to product design and development and to processes for handling third-party vulnerability reports. These consent decrees also added a new requirement: to assess the adequacy of employee training and management related to "secure engineering and defensive programming."

Many of these requirements would recur in other consent decrees for companies developing consumer-facing software applications like Snapchat, ASUSTeK, and Uber. The Uber order added more specificity to some of these requirements, including, "secure software design, development, and testing, including access key and secret key management and secure cloud storage," and "review, assessment, and response to third-party security vulnerability reports, including through a 'bug bounty' or similar program."

5. Personal Liability for Executives

GMR Transcription Services (2014), BLU Products (2018), InfoTrax (2020), Support King (2020), Drizly (2023)

In select cases, the first of which was settled in 2014, the FTC named not only companies but their C-suite level executives—including chief executive officers (CEOs), presidents, and vice presidents—as individual defendants in the consent decree.[128] This standard of liability centers around the executive having authority to "control" or "participate in" the company's information security practices.[129] In each of these cases the FTC provides evidence of the executives' culpability ranging from "not implement[ing], or properly delegate[ing] the responsibility to implement, reasonable information security practices" to an executive having "reviewed and approved" the corporation's information security policies.[130]

In these consent decrees, the FTC includes specific stipulations that the individual executive must carry out, in addition to those that the corporation is subject to. These practices include:

- For twenty years following the order, for any business that the executive is the majority owner or controls directly or indirectly, the executive must deliver a copy of the consent decree to all principles, officers, directors, and LLC managers and members, all employees with managerial responsibilities, and any new business entity.
- One year following the order, the executive must submit a compliance report to the FTC including their telephone numbers and all physical, postal, email, and internet addresses; identify all business activities; describe in detail their involvement in each business activity; and submit a compliance notice within fourteen days on changes in the executive's name, address, and title or role in a business activity.
- Complete required recordkeeping for any business that the executive is a majority owner in or controls directly or indirectly for twenty years following the consent decree.
- For ten years following the order, the individual must report to the FTC any change in name, address, or role in a business activity on the basis that the individual is an employee or has "ownership experience" and "direct or indirect control."[131]

Additionally, in the FTC's 2023 case against online alcohol marketplace Drizly and CEO James Cory Rellas, the commission required him to implement an information security program at any future company that collects

[127] See Appendix 1: Fandango Order; Credit Karma Order.

[128] See Appendix 1: Drizly Order.

[129] See Appendix 1: Support King Order; Drizly Order; BLU Products Order; InfoTrax Order; GMR Transcription Services Order.

[130] See Appendix 1: InfoTrax Order.

[131] See Appendix 1: Support King Order.

consumer information of more than twenty-five thousand people where he is the majority owner, CEO, or a senior officer for ten years following the order.[132]

6. Struck Down

LabMD (2018)

In 2005, an employee at the medical testing company LabMD downloaded a peer-to-peer file sharing application, unintentionally exposing a file on their computer that contained the health and personal information of 9,300 patients. In 2008, another company, Tiversa, obtained the file and took it to LabMD, requesting payment in exchange for fixing the vulnerability; when LabMD declined, Tiversa took the file to the FTC.[133]

Following an investigation in 2013, the FTC issued an administrative complaint against LabMD alleging that it had engaged in unfair practices because its failure to uphold reasonable cybersecurity practices led to the exposure of sensitive consumers data. The consent decree that the FTC proposed looked no different than those that had come before, including stipulations to establish a comprehensive information security program.

However, unlike almost every company before it, LabMD chose to challenge the case rather than settle. Upon review, an administrative law judge dismissed the case, stating that the FTC had failed to show that the exposure of consumer information caused or could potentially cause consumer injury—a requirement for unfairness cases, which must pertain to practices that "cause or [are] likely to cause substantial injury to consumers"—especially since there was no evidence that anyone other than Tiversa had accessed the file.[134] Appealing the decision in 2016, the FTC reversed the judge's dismissal and reopened the case, holding that the exposure of the information constituted a privacy harm that provided sufficient basis for it to bring an unfairness claim—regardless of whether or not it could be linked later to more tangible harms such as identity theft.[135]

LabMD then petitioned the Eleventh Circuit to review the FTC's decision. Following their review, in 2018, the Eleventh Circuit court vacated the FTC decree, determining that it was unenforceable because of its lack of specificity. The court found that a fundamental flaw with the order was that it "does not instruct LabMD to stop committing a specific act or practice," and suggested that the FTC did not have the right to force LabMD to "overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[136]

Because the court's ruling hinged solely on the enforceability of the consent decree, it avoided taking an explicit stance on whether the harm that the FTC cited as the basis for its action—the privacy harm—was sufficient to form the basis for an unfairness complaint. In response, the FTC would continue to bring these kinds of cases while changing its approach to the mandatory information security programs required within consent decrees.

7. Specificity and Flexibility

Fourteen Cases (2019–24)

In the wake of the LabMD case, the FTC publicly stated that it would respond to the case—and seek to more generally improve its data security-related consent decrees—by intentionally increasing the specificity of the security practices required.[137] The fourteen consent decrees in this dataset adjudicated after the LabMD decision are significantly more detailed and specific, with many new requirements. The updated consent decrees contain more requirements for respondents to document their plans, practices, and assessments, including a cadence for doing so (every twelve months or after a security incident). Nine of the fourteen consent decrees specify that the security program must be established and implemented within a certain timeframe—ranging from 30 to 180 days after the order is issued.[138]

The updated consent decrees also contain specific safeguards that companies must implement, often related to the security failure they experienced. For example, different

[132] See Appendix 1: Drizly Order.

[133] Douglas Meal, Michelle Visser, and David Cohen, "Key Takeaways from LabMD: The Implications May Be Broader Than You Think," *Bloomberg Law,* December 2018, https://www.bloomberglaw.com/external/document/XBJH6ROS000000/data-security-professional-perspective-key-takeaways-from-labmd-.

[134] Meal, Visser, and Cohen, "Key Takeaways from LabMD."

[135] Gabe Maldoff, "LabMD and the New Definition of Privacy Harm," International Association of Privacy Professionals, August 22, 2016, https://iapp.org/news/a/labmd-and-the-new-definition-of-privacy-harm.

[136] Meal, Visser, and Cohen, "Key Takeaways from LabMD."

[137] Andrew Smith, "New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers," *Federal Trade Commission*, January 6, 2020, https://www.ftc.gov/business-guidance/blog/2020/01/new-and-improved-ftc-data-security-orders-better-guidance-companies-better-protection-consumers.

[138] See Appendix 1: Zoom Order; Global Tel*Link Order; Blackbaud Order; 1Health.io Order; Ring Order, Chegg Order; Drizly Order; Cafe Press Order; SkyMed Order.

consent decrees from this time period included requirements to provide automatic firmware updates,[139] to detect unknown file uploads,[140] to rate-limit log-in attempts,[141] and to encrypt specific categories of data.[142]

Some of the most common practices required include:

- Conduct routine penetration testing (twelve out of fourteen cases)[143]
- Implement data access controls (eight out of fourteen cases)
- Log and monitor access to sensitive information (seven out of fourteen cases)
- Implement multifactor authentication (six out of fourteen cases)
- Conduct code review (three out of fourteen cases)

Yet, these new consent decrees preserve two of the most fundamental requirements from the prior generation of FTC consent decrees: that the defendant, on a regular cadence, must “assess and document [...] reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of Personal Information within the[ir] possession, custody, or control” and “design, implement, maintain, and document safeguards that control for the internal and external risks identified.”[144]

8. Maintain a Data Retention Program

Chegg (2023), Drizly (2023), Blackbaud (2024)

In three of the most recent consent decrees contained in this dataset, the FTC included a new provision: a requirement to establish a data retention program. As part of this program, the consent decree specifically requires a publicly available retention schedule for consumer information that must include:

- The purpose of information collection
- The business’ need for retaining the information
- The timeframe for deletion of the information

Even though the FTC had cited a failure to discard no-longer-needed consumer data as an unreasonable practice in complaints from before these three cases, these were the first examples of the FTC specifically requiring a data retention program in the resulting consent decrees. This suggests a concerted effort by the agency to foreground data minimization as a core part of a comprehensive information security program. Perhaps it is a recognition of the fact that this was not a common component of the risk-based programs that businesses were implementing.

[139] See Appendix 1: D-Link Order.

[140] See Appendix 1: InfoTrax Order.

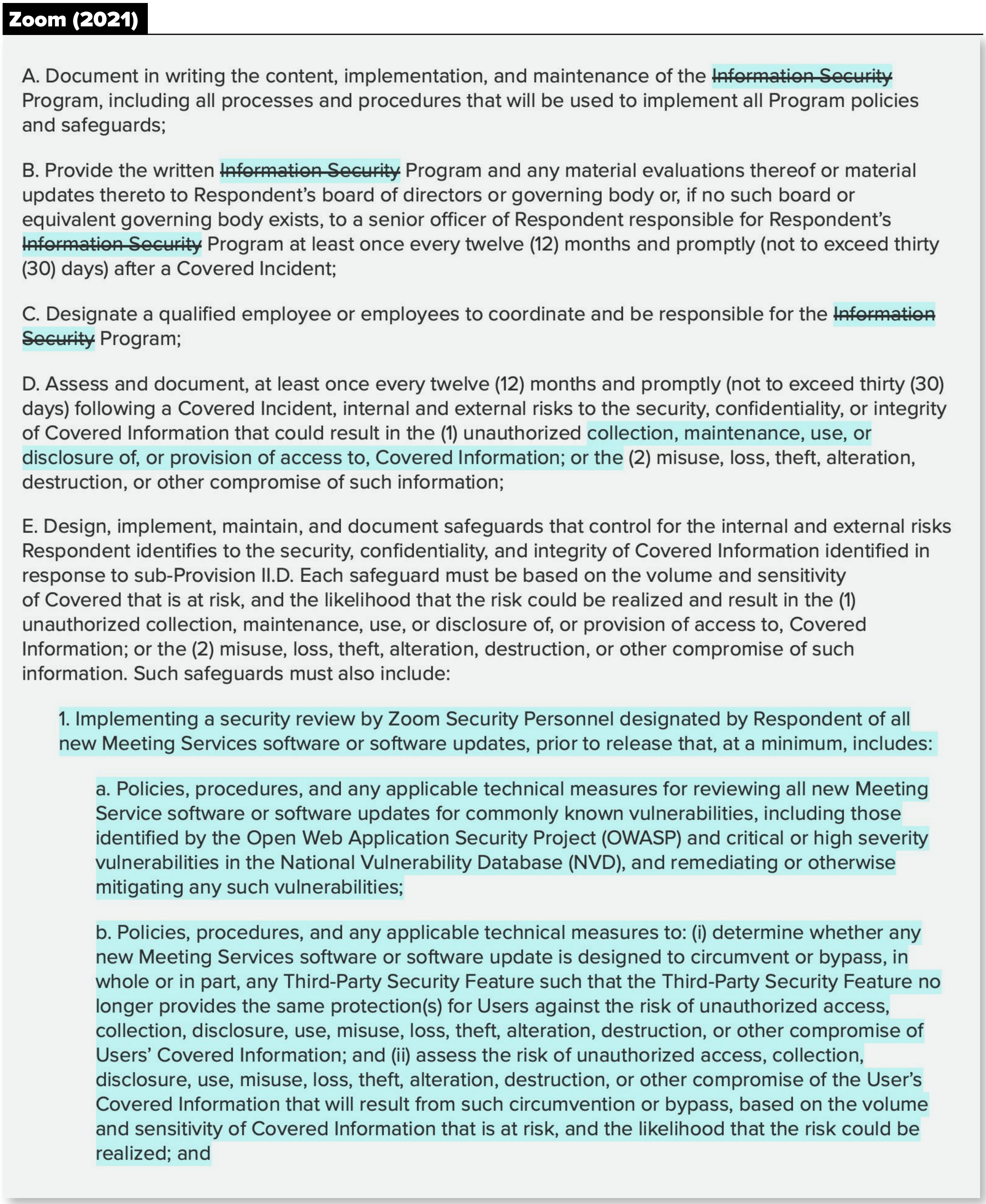
[141] See Appendix 1: Zoom Order.

[142] See Appendix 1: SkyMed Order.

[143] See Appendix 1: InfoTrax Order; Tapplock Order; SkyMed Order; Support King Order; Drizly Order; Chegg Order; Ring Order; Health.io Order; Residual Pumpkin (CafePress) Order; Blackbaud Order; GlobalTelLink Order.

[144] See Appendix 1: Global Tel*Link Order.

Figure 7: Zoom Consent Decree



Zoom (2021)

A. Document in writing the content, implementation, and maintenance of the ~~Information Security~~ Program, including all processes and procedures that will be used to implement all Program policies and safeguards;

B. Provide the written ~~Information Security~~ Program and any material evaluations thereof or material updates thereto to Respondent’s board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent’s ~~Information Security~~ Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

C. Designate a qualified employee or employees to coordinate and be responsible for the ~~Information Security~~ Program;

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the security, confidentiality, and integrity of Covered Information identified in response to sub-Provision II.D. Each safeguard must be based on the volume and sensitivity of Covered that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:

1. Implementing a security review by Zoom Security Personnel designated by Respondent of all new Meeting Services software or software updates, prior to release that, at a minimum, includes:

    a. Policies, procedures, and any applicable technical measures for reviewing all new Meeting Service software or software updates for commonly known vulnerabilities, including those identified by the Open Web Application Security Project (OWASP) and critical or high severity vulnerabilities in the National Vulnerability Database (NVD), and remediating or otherwise mitigating any such vulnerabilities;

    b. Policies, procedures, and any applicable technical measures to: (i) determine whether any new Meeting Services software or software update is designed to circumvent or bypass, in whole or in part, any Third-Party Security Feature such that the Third-Party Security Feature no longer provides the same protection(s) for Users against the risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users’ Covered Information; and (ii) assess the risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of the User’s Covered Information that will result from such circumvention or bypass, based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized; and

case-specific changes

Zoom (2021)

c. Policies, procedures, and any applicable technical measures so that Respondent will not implement any new Meeting Services software or software update that has been identified under Part II.E.1.b(i) of this Order as designed to circumvent or bypass a Third-Party Security Feature, unless: (i) Zoom Security Personnel determine that the bypass or circumvention does not create a material risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users’ Covered Information; or (ii) Respondent implements security measure(s) that offset or otherwise mitigate the risk(s) of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users’ Covered Information that were identified under Part II.E.1.b(ii) of this Order;

2. Implementing a vulnerability management program that includes: a. Conducting vulnerability scans of Respondent’s networks and systems on at least a quarterly basis; and 6 b. Policies, procedures, and any applicable technical measures for remediating or otherwise mitigating any critical or high severity vulnerabilities promptly (but in no event later than thirty (30) days after the vulnerability is detected), unless Respondent documents its rationale for not doing so;

3. Implementing a default, randomized naming convention for recorded Meetings that are to be stored on Users’ local devices, and instructing Users to employ a unique file name when saving such recorded Meetings;

4. Policies, procedures, and any applicable technical measures to: (a) systematically classify and inventory Covered Information in Respondent’s control; (b) log and monitor access to repositories of Covered Information in Respondent’s control; and (c) limit access to Covered Information by, at a minimum, limiting employee and service provider access to Covered Information to what is needed to perform that employee or service provider’s job function;

5. Data deletion policies, procedures, and any applicable technical measures, including validating that all copies of Covered Information identified for deletion are deleted within thirty-one (31) days;

6. Policies, procedures, and any applicable technical measures designed to reduce the risk of online attacks resulting from the misuse of valid Credentials by unauthorized third parties, including: (a) requiring Users to secure their accounts with strong, unique passwords; (b) using automated tools to identify non-human login attempts; (c) rate-limiting login attempts to minimize the risk of a brute force attack; and (d) implementing password resets for known compromised Credentials;

7. Regular security training programs, on at least an annual basis, that are updated, as applicable, to address internal or external risks identified by Respondent under subProvision II.D of this Order, and that include, at a minimum: a. Security awareness training for all employees on Respondent’s security policies and procedures, including the requirements of this Order and the process for submitting complaints and concerns; and b. Training in secure software development principles, including secure engineering and defensive programming concepts, for developers, engineers, and other employees that design Respondent’s products or services or that are otherwise responsible for the security of Covered Information;

case-specific changes

Zoom (2021)

8. Technical measures to monitor all of Respondent’s networks, systems, and assets within those networks to identify anomalous activity and/or data security events on Respondent’s network, including unauthorized attempts to exfiltrate Covered Information from Respondent’s networks;

9. Incident response policies, procedures, and any applicable technical measures, including centralized log management and documenting remedial security actions;

10. Technical measures designed to safeguard against unauthorized access to any network or system that stores, collects, maintains, or processes Covered Information, such as properly configured firewalls; properly configured physical or logical segmentation of networks, systems, and databases; and securing of remote access to Respondent’s networks through multi-factor authentication or similar technology except for when accessing such networks is for the purpose of using Meeting Services; and

11. Protections, such as encryption, tokenization, or other same or greater protections, for Covered Information collected, maintained, processed, or stored by Respondent, including in transit and at rest;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, and integrity of Covered Information, and modify the ~~Information Security~~ Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include ~~vulnerability testing of each of Respondents’ network(s) once every four months and promptly after a Covered Incident~~ penetration testing of Respondent’s network at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Information sufficient to address the internal and external risks to the security, confidentiality, or integrity of ~~Personal~~ Covered Information;

I. Consult with, and seek appropriate guidance from, independent, third-party experts on data protection in the course of establishing, implementing, maintaining, and updating the ~~Information Security~~ Program; and

J. Evaluate and adjust the ~~Information Security~~ Program in light of any changes to Respondent’s operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision II.D of this Order, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of the ~~Information Security~~ Program or any of its individual safeguards. At a minimum, Respondent must evaluate the ~~Information Security~~ Program at least once every twelve (12) months and modify the Information Security Program as necessary based on the results.

case-specific changes

Analysis: Commonalities and Differences in Information Security Programs

These forty-seven consent decrees illustrate the FTC's evolving conception of a comprehensive security program and reveal trends in the ways that the agency has utilized both broad and specific requirements to advance data security practices at responding companies.

Trend: Setting a Standard

The FTC's consistent use of the same baseline requirements in the information security programs suggests a desire to define a set of broad norms for reasonable information security programs that go beyond the specific security failures that triggered the complaints. This approach is particularly notable in consent decrees like the one related to Guidance Software, which added an additional element to the mandatory information security program that had little relation to the particular facts of the Guidance Software case. And, it is precisely this practice which landed the agency in hot water in the LabMD case: the court suggested that the FTC consent decrees did not seek to prevent companies from undertaking particular acts or practices, but instead sought to force companies to overhaul their security programs wholesale.

Trend: The Benefits of a Risk-Based Approach

Across all the consent decrees, the FTC articulates a foundational requirement for businesses to identify risks and implement appropriate safeguards. This construction allows the decrees to avoid laying out a static set of activities that would be sufficient to keep a company wholly secure, which would require a great deal of specialized knowledge about its technologies, networks, and data, and would be likely to become outdated during the twenty years of the decree's application. Even after the LabMD case forced the FTC to be more specific in the practices it requested from defendants, consent decrees continued to require respondents to identify and mitigate risks in addition to implementing other more specific controls. Taken together, these factors suggest that risk-based approaches and mitigations have an enduring place in the FTC's conception of how to construct an information security program.

Trend: The Benefits of Specificity

At the same time, the decrees are not limited to this requirement. Several decrees—even before the LabMD case required more specificity—supplemented the basic decree with carefully delineated provisions and requirements, such as the obligation to oversee service providers and, in the case of companies developing software, to use secure programming practices and application testing. That the consent decrees have evolved in this way over time suggests that the FTC might have seen evidence, in its work to supervise consent decrees, that general risk mitigation requirements should be married with more specific practices applicable to the company and its activities. Later evolutions, such as the addition of a required program for data minimization, also suggest that the agency might have viewed specificity as a better way to advance practices that contribute to security but that might not otherwise be prioritized by companies under a simple risk-based approach.

Conclusions

Consumers are Our Business

The FTC's consumer protection mandate both broadens and limits its power in the cyber domain. The scoping function for the FTC's cyber enforcement is consumer protection; for cases brought on the basis of unfairness, this hinges upon the agency's contention that bad data security practices cause or are likely to cause harm to consumers. This is a superpower—where consumers go, the agency can follow, without restrictive focus on a single class or instance of technology. These potential repercussions or harms to consumers can range from financial injury (fraudulent transactions) to emotional distress (public exposure of sensitive information)[145] to threats to safety (consumer location information or gender identity),[146] encompassing a range of companies and types of data. The FTC can tackle large companies when their practices have the potential to harm many; it can focus on small companies whose practices are egregiously harmful; and it can apply the most stringent scrutiny to companies that process the most sensitive data.

Giving an agency a broad mandate to protect consumers is a powerful way to allow them to continue to evolve their standards in the face of an ecosystem both as rapidly evolving and as heterogenous as cybersecurity. No set of standards drafted in 2002 would be likely to encompass the security failures that occurred in the FTC's 2024 case against Global Tel*Link Corporation—including a failure to employ a perimeter firewall, log monitoring solution, and automated monitoring software.[147] This broad mandate allows the agency to reach across heterogenous technology projects, from massive cloud infrastructure to consumer apps to enterprise data storage systems to Internet of Things devices, and to update the kinds of practice it pursues alongside the rapid evolution in the underlying technologies that must be secured.

However, the question of harm is also a potential Achilles' heel for the FTC. Whether judges will agree with the FTC's contention in the LabMD case, that privacy harms form sufficient basis for its unfairness actions, is still relatively open. In 2023, a judge rejected the FTC's case against Kochava, a location data broker, because the agency had failed to show how the company's practices could cause "substantial injury" to consumers.[148] In February 2024, the judge allowed the FTC's case to proceed after the agency amended its complaint and enumerated the potential harms that could befall consumers as the result of the data the company sold. However, the final status of the case has yet to be determined—and a ruling on whether or not the FTC can treat privacy harms as sufficient to create the basis for a claim of unfairness will have substantial ripple effects on the agency's efficacy as an enforcer in the data security space. Even beyond the specific focus of the FTC, the question about the right way to think about privacy harms has dogged the US privacy conversation.[149]

Generality and Specificity

The consent decrees within this dataset provide a model of how the FTC has combined general and specific obligations in the information security programs it requires companies to uphold. Specific requirements makes it easy to verify whether a company has a control in place and to show wrongdoing when they lack it, and can help advance certain behaviors that might not otherwise be a part of companies' risk mitigation menu, such as data minimization. After the LabMD case, the agency itself stated that the added specificity would make it easier to enforce its decrees.[150] Yet, even after LabMD, the FTC has also maintained in its consent decrees certain general requirements—e.g., that companies identify risks to the data they hold and implement controls and protections for those risks appropriate to their size and activities. This requirement creates a flexible obligation that can adapt alongside changing best practices in the cybersecurity field. The ever-evolving list of bad practices evident in the FTC complaints—including new failures such as to secure cloud credentials or failures to enable multifactor authentication—suggests that enforcement structures in this space will need a mechanism to continuously evolve if they are to keep pace with the evolution of

[145] See Appendix 1: Global Tel*Link Complaint.

[146] See Appendix 1: Global Tel*Link Complaint.

[147] See Appendix 1: Global Tel*Link Complaint.

[148] Suzanna Smalley, "Judge allows case against geolocation data broker Kochava to proceed," *The Record*, February 5, 2024, https://therecord.media/judge-allows-ftc-case-against-kochava-data-broker-to-proceed.

[149] Danielle Keats Citron and Daniel J. Solove, "Privacy Harms," Boston University Law Review (2022), 793.

[150] Smith, "New and improved FTC data security orders."

cybersecurity best practice. (And perhaps one even faster than multi-year federal rule-making processes.)

To incentivize the adoption of specific behaviors or controls while preserving flexibility, policymakers seeking to design legal structures to advance—whether for companies processing consumer data, or for those selling software—might consider these kinds of blended approaches. Specific lists of best practices, perhaps even drawn from existing examples of legal standards for unreasonable cybersecurity behavior, could provide a set of known practices that companies must implement or avoid; these specific practices could be paired with broader obligations for each company to assess and appropriately mitigate the risks they face.

Certain proposed data security frameworks, like the new American Privacy Rights Act, adopt this kind of general-and-specific structure: the bill combines a requirement for entities to adopt "reasonable" cybersecurity measures based on their size and activities with a requirement for them to adopt a few specific practices including assessing vulnerabilities, deleting unnecessary data, and training their employees. While the bill allows the FTC to develop process-based regulations for this section's implementation, there is no structure by which the agency can outline specific required practices or controls for companies. Instead, much would hinge on the question of how enforcers, judges, and companies themselves interpret the question of reasonableness.

I Find You Unreasonable

The FTC's construction of reasonableness provides a model of how companies' claims about their security behavior can be assessed: against the broader state of knowledge within a field, against expert warnings and past failures that should serve to inform companies of the risks they face and the precautions they must take. Evaluating companies against what is widely known or widely adopted within the field provides a neat way to respect the fact that different technologies face different kinds of risks and different types of data processing activities—or different types of data itself—that demand different levels of risk mitigation. While these standards are not perfectly fixed, necessitating elements of judgement, they at least provide a measuring stick that companies can use to assess their own security posture. While flexibility creates its own challenges in terms of both compliance and enforcement, it will be challenging to define any static, single standard that can tackle an ecosystem as sprawling as consumer cybersecurity.

The debate over software liability in the United States is raging at this moment,[151] with a key question being how to define standards that will be adaptive over time while providing businesses a measure of certainty about their obligations (and avoiding an overabundance of litigation without corresponding gains in security). Several of the cases in the dataset pertain to questions about the reasonable design of software systems. The kinds of unreasonable behavior outlined within could play a role in defining certain baseline standards associated with a federal software liability regime; perhaps such a regime could even make use of a federal agency already designed and primed to handle questions of reasonable behavior with respect to consumer harm and cybersecurity.

On the FTC

The consistency of the FTC's cyber enforcement actions is notable, even as administrations have changed and FTC commissioners have come and gone. New commissioners have brought shifts in focuses to be sure: take, for example, the move to address mobile and Internet of Things devices under Edith Ramirez, and current Chair Lina Khan's prioritization of actions against data brokers. Yet, the lack of gaps or manifest periods of total de-prioritization of cyber enforcement is remarkable.

At the same time, despite its consistency, the relatively small size of this dataset is notable too: the FTC has typically resolved only a few cyber enforcement cases each year. What would you do if you had just a few cases each year to address cybersecurity standards and failures for new and unregulated technologies that were causing potential harm to consumers? How would you prioritize and adapt? This is the question the FTC has had to consider for the past twenty years, with just a few dozen staff in its Division of Privacy and Identity Protection.

In the years since 2002, when the first action in this dataset was brought, the technology landscape has changed drastically. Major social media sites Facebook, YouTube, Instagram, Snapchat, and TikTok emerged; Amazon, Google, and Microsoft began offering cloud computing services; the iPhone was born; and meaningful consumer-facing generative artificial intelligence services have emerged. These innovations have changed the ways in which software is used and users' digital data is collected, stored, and processed. Each case that the FTC brings requires substantial resources, from investigation to filing and negotiations to supervising companies' compliance with eventual consent decrees. Thus, the agency must

[151] Maia Hamin, Trey Herr, and Stewart Scott, "Three Questions on Software Liability," *Lawfare,* September 7, 2023, https://www.lawfaremedia.org/article/three-questions-on-software-liability.

choose exemplar cases, hoping that other companies—those in the same industry, or processing the same kinds of data, or lacking the at-issue protections—get the message.

In addition to creating challenges in bringing new cases, the extremely limited number of staff in the FTC's Division of Privacy and Identity Protection may also imperil the oversight and enforceability of the consent decrees into which the agency does enter. Because most consent decrees last for twenty years, the FTC has only just finished the monitoring period for some of its very first cases covered in this analysis. Not only does technology grow more complex and more embedded into many of the systems with which consumers must interact—the sheer administrative burden of overseeing existing decrees grows. The question of how to measure the FTC's enforcement capacity and the impact of changes in that capacity is an important question and one for future work.

Beyond capacity, in April of 2021, the Supreme Court stripped the FTC of its authority to seek monetary redress for first-time violations of Section 5a under Section 13b, in AMC Capital Management, LLC, v. FTC.[152] The fact that companies cannot face fines for UDAP violations may reduce their incentives to proactively implement cybersecurity safeguards, lessening the disciplinary power that these cases have over the broader market. While there exist alternative pathways for the FTC to seek redress, they are arduous, prompting calls from FTC commissioners for legislation that would give the FTC the legal authority to seek monetary redress for Section 5a violations in federal court.[153]

Another challenge to the FTC's ability to create lasting change in the cybersecurity ecosystem may come in the form of future litigation. The FTC has already faced two major legal challenges to their cybersecurity authority—Wyndham v. FTC in 2015, in which the Third Circuit upheld the FTC's authority to police cybersecurity-related violations of Section 5a, and LabMD in 2018—there is a real possibility that companies may increasingly start to challenge the FTC's authority. One avenue for challenges that could particularly threaten the FTC's UDAP cyber enforcement is the question of whether privacy harms form a sufficient basis for an unfairness claim, as addressed in the previous section—any finding that they do not would imperil the very basis of many of the FTC's enforcement actions in the cyber space, since these actions tend to hinge upon the theft or exposure of consumer data.

To be sure, the FTC has done a lot with little: with a mandate from 1914 and minimal staff members, in just forty-seven cases, they have litigated a variety of harmful practices from the indefinite retention of consumers personal information[154] to the storage of AWS cloud bucket credentials in GitHub repositories.[155] However, the question remains whether this mandate and capacity can keep pace with the continued evolution of digital technologies. Without more explicit consumer data protection authorities, the FTC will need to continue standard-setting through its slow drumbeat of UDAP cases, rather than being able to set proactive standards and requirements. Without more resources and staff, there will continue to be real capacity constraints on the volume of cases and practices that the agency can pursue. Without the ability to levy penalties for violations, companies may see little incentive to pay heed to the evolving standards within the FTC's complaints and decrees. And without legal clarification, a new court decision could imperil the very foundations of its enforcement actions to date.

Without the clear specification and enforcement of baseline security practices, consequential failures in the security of digital technologies will continue to stack up, even as more and more of the world is dependent on digital infrastructure. In the meantime, and in the continued absence of a wider liability regime, the FTC works quietly along, pursuing unfair and deceptive data security practices and shaping a set of standards for consumer data security with the tools they have at hand.

[152] AMG Capital Management, LLC v. Federal Trade Comm'n, 593 U.S. ___ (2021).

[153] *Hearing on Oversight of the Federal Trade Commission, Before the Comm. on Commerce, Science, and Transportation*, 116th Cong. 6. (2020) (statement of the Federal Trade Commission).

[154] See Appendix 1: Life is Good Complaint.

[155] See Appendix 1: Drizly Complaint.

Appendix

Table 1: Short form names and full citations

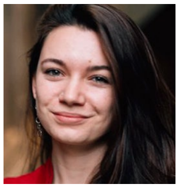
Short Form Name	Citation
Ashley Madison Complaint	Complaint, Ruby Corp., Ruby Life Inc. d/b/a AshleyMadison.com, ADL Media Inc. (Dec 14, 2016)
ASUSTeK Complaint	Complaint, ASUSTeK Inc., FTC File No. 142-3156, (Jul 18, 2016)
BJ’s Complaint	Complaint, BJ’s Wholesale Club, Inc., FTC File No. 042-3160, (Sep 20, 2005)
Blackbaud Complaint	Complaint, Blackbaud, Inc., FTC File No. 052-3094, (Jun 15, 2011)
Blackbaud Order	Decision and Order, Blackbaud, Inc., FTC File No. 052-3094, (Jun 15, 2011)
BLU Products Complaint	Complaint, BLU Products, Samuel Ohev-Zion., FTC File No. 172-3025, (Sep 6, 2018)
BLU Products Order	Decision and Order, BLU Products, Inc., Samuel Ohev-Zion, FTC File No. 172-3025, (Sep 6, 2018)
Card Systems Solutions Complaint	Complaint, Card Systems Solutions, Inc., FTC File No. 052-3148 (Sep 5, 2006)
Ceridian Complaint	Complaint, Ceridian Corporation, FTC File No. 102-3160 (Jun 8, 2011)
Chegg Complaint	Complaint, Chegg, Inc., FTC File No. 202-3151, (Jan 25, 2023)
Chegg Order	Decision and Order, Chegg, Inc., FTC File No. 202-3151, (Jan 25, 2023)
Compete Complaint	Complaint, Compete, Inc., FTC File No. 102-3155, (Feb 20, 2013)
Credit Karma Complaint	Complaint, Credit Karma, FTC File No. 202-3138, (Aug 19, 2014)
Credit Karma Order	Decision and Order, Credit Karma, FTC File No. 202-3138, (Aug 19, 2014)
D-Link Complaint	Complaint, D-Link Systems, Inc., FTC File No. 052-3094000-39, (Jul 2, 2019)
D-Link Order	Decision and Order, D-Link Systems, Inc., FTC File No. 052-3094000-39, (Jul 2, 2019)
Dave & Busters	Complaint, Dave & Busters, Inc., FTC File No. 082-3153 (May 20, 2010)
Drizly Complaint	Complaint, Drizly LLC, James Cory Rellas, FTC File No. 202-3185 (Oct 3, 2012)
Drizly Order	Complaint, Drizly LLC, James Cory Rellas, FTC File No. 202-3185 (Jan 10, 2023)
DSW Complaint	Complaint, DSW Inc., FTC File No. 052-3096 (Aug 1, 2006)
EPN Checknet Complaint	Complaint, EPN Inc. d/b/a Checknet, Inc. FTC File No. 112-3143 (Aug 1, 2006)
Fandango Complaint	Complaint, Fandango, LLC, FTC File No. 132-3089 (Aug 13, 2014)
Fandango Order	Decision and Order, Fandango, LLC, FTC File No. 132-3089 (Aug 13, 2014)
Genica Complaint	Complaint, Genica Corporation and compgeeks.com d/b/a Computer Geeks Discount Outlet and Geeks.com, FTC File No. 082-3133, (Mar 16, 2009)
Global Tel*Link Complaint	Complaint, Global Tel*Link Corp., FTC File No. 212-3012 (Feb 23, 2024)
Global Tel*Link Order	Decision and Order, Global Tel*Link Corp., FTC File No. 212-3012 (Feb 23, 2024)
GMR Transcription Services Complaint	Complaint, GMR Transcription Services, Inc., Ajay Prasad, Shreekant Srivastava FTC File No. 122-3059 (Aug 14, 2014)
GMR Transcription Services Order	Decision and Order, GMR Transcription Services, Inc., Ajay Prasad, Shreekant Srivastava FTC File No. 122-3059 (Aug 14, 2014)

Short Form Name	Citation
Guess Complaint	Complaint, Guess?, Inc. and Guess.com, Inc., FTC File No. 052-3057 (Jul 13, 2003)
Guidance Software Complaint	Complaint, Guidance Software, Inc., FTC File No. 052-3094062-3057, (Mar 30, 2007)
Guidance Software Order	Decision and Order, Guidance Software, Inc., FTC File No. 052-3094062-3057, (Mar 30, 2007)
1Health.io Order	Decision and Order, 1Health.io/Vitagene, FTC File No. 1923170, (Sept 7, 2023)
HTC America Complaint	Complaint, HTC America, Inc., FTC File No. 122-3049, (Jun 25, 2013)
HTC America Order	Decision and Order, HTC America, Inc., FTC File No. 122-3049, (Jun 25, 2013)
InfoTrax Complaint	Complaint, InfoTrax Systems, L.C, Mark Rawlins, FTC File No. 162-3130, (Dec 13, 2019)
InfoTrax Order	Decision and Order, InfoTrax Systems L.C, Mark Rawlins Inc., FTC File No. 162-3130, (Dec 13, 2019)
James V. Grago, Jr. (ClixSense) Complaint	Complaint, James V. Grago, Jr. d/b/a ClixSense.com, FTC File No. 172-3003, (Jun 19, 2019)
Lenovo Complaint	Complaint, Lenovo, Inc., FTC File No. 172-3003, (Jun 19, 2019)
Life is Good Complaint	Complaint, The Life is Good Company, FTC File No. 152-3134 (Dec 20, 2017)
LifeLock Complaint	Complaint, LifeLock Inc., Robert J Maynard, Richard Todd Davis (Mar 8, 2010).
Lookout Services Complaint	Complaint, Lookout Services, Inc., FTC File No. 102-3076, (Jun 15, 2011)
Microsoft Complaint	Complaint, Microsoft Corporation, FTC File No. 012-3240, (Dec 20, 2002)
Microsoft Order	Decision and Order, Microsoft Corporation, FTC File No. 012-3240, (Dec 20, 2002)
MTS (Tower Records) Complaint	Complaint, MTS, Inc. d/b/a Tower Records/Books/Video, Tower Direct, LLC d/b/a Towerrecords.com, FTC File No. 032-3209, (Mar 4, 2005)
Petco Complaint	Complaint, Petco Animal Supplies, Inc., FTC File No. 03203221, (Jun 15, 2011)
Reed Elsevier Complaint	Complaint, Reed Elsevier Inc and Seisint, Inc., FTC File No. 052-3094, (Aug 1, 2008)
Residual Pumpkin (CafePress) Complaint	Complaint, Residual Pumpkin Entity, LLC, FTC File No. 052-3094192, (Jan 10, 2024)
Residual Pumpkin (CafePress) Order	Decision and Order, Residual Pumpkin Entity, LLC, FTC File No. 052-3094192, (Jan 10, 2024)
Ring Complaint	Complaint, Ring LLC, FTC File No. 052-30941549, (Jun 16, 2023)
Ring Order	Decision and Order, Ring LLC, FTC File No. 052-30941549, (Jun 16, 2023)
SkyMed Complaint	Complaint, SkyMed International d/b/a SkyMed Travel and Car Rental Pro, FTC File No. 192-3140 (Jan 26, 2011)
SkyMed Order	Decision and Order, SkyMed International d/b/a SkyMed Travel and Car Rental Pro, FTC File No. 192-3140 (Jan 26, 2011)
Support King Complaint	Complaint, Support King, LLC and Scott Zuckerman, FTC File No. 192-3003, (Dec 20, 2021)
Support King Order	Decision and Order, Support King LLC and Scott Zuckerman, FTC File No. 192-3003, (Dec 20, 2021)
Tapplock Complaint	Complaint, Tapplock Corp., FTC File No. 192-3011, (May 18, 2020)
Tapplock Order	Decision and Order, Tapplock Corp., FTC File No. 192-3011, (May 18, 2020)

Short Form Name	Citation
TJX Complaint	Complaint, The TJX Companies, Inc., FTC File No. 072-3055, (Jul 29, 2008)
TRENDnet Complaint	Complaint, TRENDnet, Inc. FTC File 122-3090, (Feb 7, 2014)
Uber Complaint	Complaint, Uber Technologies, Inc., FTC File No. 152-3054 (Oct 25, 2018)
Uber Order	Decision and Order, Uber Technologies, Inc., FTC File No. 152-3054 (Oct 25, 2018)
Upromise Complaint	Decision and Order, Upromise, Inc., FTC File No. 102-3116 (Mar 27, 2012)
Wyndham Complaint	Complaint, Wyndham Worldwide Corporation Inc., File No. 052-3094, (Dec 23, 2014)
Zoom Order	Decision and Order, Zoom Video Communications, Inc., File No. 192-3167, (Feb 1, 2021)

About the Authors

Isabella Wright was a consultant and Young Global Professional with the Atlantic Council's Cyber Statecraft Initiative within the Digital Forensic Research Lab (DFRLab). She graduated from the University of California, Berkeley where she majored in history with an emphasis in the history of science and technology.



Maia Hamin is an Associate Director with the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). She works on the intersection of cybersecurity and technology policy, including projects on the cybersecurity implications of artificial intelligence, open-source software, and cloud computing. Prior to joining the Council, Maia was a TechCongress Congressional Innovation Fellow serving in the office of Senator Ron Wyden, and before that a software engineer on Palantir's Privacy and Civil Liberties team. She holds a B.A. in Computer Science from Princeton University.

Atlantic Council | Board of Directors

[redacted]

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org