iapp WHITE PAPER

From Reasonable to Particular:

The Rise of Prescriptive Technical Safeguards in FTC Settlements

By Samuel Adams, Policy Fellow at the Future of Privacy Forum*

Contents

CONTENT OVERVIEW

- A review of U.S. Federal Trade Commission settlements that have required increasingly specific remedies since the pivotal 2018 LabMD case.
- A contextualization of why certain technologies like multi-factor authentication are now stipulated in some FTC settlements.
- Should organizations begin implementing technologies promoted by the commission, even if they have not yet been stipulated in a settlement order?

Executive Summary

The FTC has taken a case-by-case approach to enforce Section 5 of the FTC Act in the digital arena. For years, FTC settlements required companies to implement comprehensive information security programs, often deploying template language that lacked requirements specifying how companies were to execute the means to the desired end: consumer privacy protections reasonably tailored to the risks.

But the 2018 LabMD case forced the FTC to rethink its approach, leading to more granular stipulated remedial measures in settlements. For example, the 2022 CafePress settlement features the first-ever requirement that a company implement multi-factor authentication using a secure third-party authentication app, a technology long promoted by the FTC to consumers and businesses to secure user access. Other privacy-enhancing technologies are likely to appear in future FTC settlements. As an illustration, we highlight recent FTC guidance on practices related to reproductive health information. Organizations should consider implementing procedural and technical measures the FTC has highlighted in its prior guidance, where appropriate.

FTC enforcement history and the 'reasonable' security standard

The FTC Act and the 'Common Law'

The FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." To enforce this prohibition, the law authorizes the Federal Trade Commission to initiate an administrative complaint, laying out its charges that the law has been violated. The respondent may either choose to settle the charges and sign a consent agreement without admitting liability, hereafter "settlement," or contest the charges. The overwhelming majority of cases brought by the FTC settle, and the Commission posts the complaints, settlements, and other pertinent documents online for public access.

The remedial measures required by the settlement documents form what two leading privacy scholars coined FTC "common law" because, like traditional common law, accumulated FTC cases informally codify information security and privacy norms and principles and, in turn, dictate baseline protections. By negative inference, FTC common law illuminates which privacy and security practices companies defending against FTC complaints, "respondents," could have implemented to avoid investigation and enforcement in the first place. FTC common law also prompts other organizations to internalize whether to implement the remedies described in settlements to comply with implied FTC baseline privacy and security protections.

But for more than a decade, FTC cases gave little insight into how respondents were supposed to implement remedial information security programs stipulated by settlements. This was the case until 2018, when a federal appeals court forced the commission to begin issuing complaints with greater specificity regarding what conduct violated the FTC Act and which technical, administrative, and policy remedies companies must implement to settle those allegations.

To understand how FTC settlements have grown in length and complexity, it is important to understand how the commission began enforcing cybersecurity violations in the early 2000s.

> ***By negative inference, FTC common law illuminates which privacy and security practices companies defending against FTC complaints, "respondents," could have implemented to avoid investigation and enforcement in the first place.***

Eli Lilly: A gamechanger

The story began with the 2002 administrative case against Eli Lilly, the maker of Prozac. Until then, it was unclear how the FTC would regulate consumer protection in the nascent and growing internet environment using the 108-year-old FTC Act. Eli Lilly established an important framework that all future FTC cases would replicate. Decades later, the vague implementation requirements for the respondent to achieve comprehensive security would come under judicial scrutiny.

The Eli Lilly case began when an employee at the company unintentionally disclosed personal information related to consumers' use of a company-operated website, Prozac.com. In the complaint, the FTC alleged that the disclosure caused the company to break the website's stated promises that it would "respect the privacy of [website] visitors," "maintain our guests' privacy," and "protect the confidentiality" of consumer information. In the view of the FTC, Eli Lilly's alleged failure to live up to these statements constituted a violation of the FTC Act.

> ***Eli Lilly established an important framework that all future FTC cases would replicate.***

Eli Lilly settled the charges in a deal where the company consented to overhaul its information security program and practices to prevent another similar incident, but the story did not end there. The settlement went further than preventing an identical violation because it imposed a comprehensive restructuring of the company's data practices by requiring technical, administrative, and physical safeguards. These included employee training, risk assessments, annual reviews, periodic adjustments to the program, and the requirement that the company maintains the information security program for 20 years.

The case was significant because it formed the genesis for the FTC's extant enforcement framework. Even though the complaint alleged a single incident of failed security, the FTC's investigation and eventual settlement evaluated Eli Lilly's cybersecurity practices on a wider scale than just the underlying incident. But the settlement did not detail how Eli Lilly was to achieve the required outcome — that is, rather than identifying the specific components of "employee security training" necessary to avoid another violation, the settlement left those implementation decisions to the company.

The 'reasonable' security era

A 2005 case first saw the FTC begin including reasonableness as a standard of its mandated remedial information security programs. This requirement endured until a federal appeals court balked at the vagueness of the standard.

The BJ's Wholesale Club case was the first to include the reasonableness standard. The complaint alleged several instances the retailer failed to practice reasonable security, including failing to encrypt consumer information in transit across its wireless network or stored on company computers, storing consumer information behind strong usernames and passwords, not limiting access to its wireless networks, not using measures to detect unauthorized access to its networks, and storing data longer than was necessary.

Borrowing from the Eli Lilly framework, the BJ's settlement required the retailer to implement and maintain a comprehensive information security program with remedies wider in scope than the circumstances that caused the underlying violation. But what set it apart from Eli Lilly was the requirement the BJ's program be "reasonably designed" to protect consumer data and that the company implement "specific safeguards" to mitigate the risk identified in the mandatory risk assessment.

But despite the addition of the reasonableness standard, the BJ's settlement still said little about how the company was supposed to

achieve the desired outcome. Just like the Eli Lilly settlement, the onus was on BJ's to develop its own definitions of reasonable security, which the company could base on anything from industry norms, the specific allegations in the complaint, or a nascent version of what would later be referred to as the FTC common law of data security.

> ***But what set it apart from Eli Lilly was the requirement the BJ's program be "reasonably designed" to protect consumer data and that the company implement "specific safeguards" to mitigate the risk identified in the mandatory risk assessment.***

Leaving it up to BJ's reflected an intentional aspect of the FTC's case-by-case enforcement approach because different organizations face different risks. The security practices "reasonably designed" for BJ's circumstances may not be appropriate for a competitor. By contrast, adopting a one-size-fits-all approach requiring, for example, a type of encryption generally accepted as secure in 2005 that would later become obsolete could leave respondents vulnerable to repeated violations, especially given that many FTC settlements are binding for 20 years. Thus, the standard that programs be "reasonably designed" to protect consumer information was partly intended to guide respondents to implementing comprehensive security programs that would remain flexible to shifting risks and security environments.

The Inflection Point

LabMD and the end of the 'reasonableness' standard

Although the vast majority of respondents settle, some respondents fight the FTC in federal court. One such litigation involving laboratory company LabMD resulted in the end of the FTC's often vague remedial measures — and the reasonableness standard — paving the way for the more granular settlements that have become the norm of late.

In 2013, a cybersecurity research firm discovered files belonging to LabMD were publicly available through a peer-to-peer file-sharing program, exposing the personal information of more than 9,000 consumers to a high risk of unauthorized access. The FTC alleged the company failed to implement reasonable security practices such as intrusion detection systems, file integrity monitoring, firewall traffic monitoring, security training for employees. It also alleged a failure of risk-reducing data minimization practices because the company had been storing consumer information longer than necessary.

LabMD appealed the FTC's findings to a federal appeals court, arguing among other issues, the commission's allegation that LabMD had failed to employ reasonable security was too vague as to be enforced. In 2018, a federal court of appeals sided with LabMD, ruling the term "reasonable" was "devoid of any meaningful standard" and that the FTC's approach to the case "mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished."

One such litigation involving laboratory company LabMD resulted in the end of the FTC's often vague remedial measures — and the reasonableness standard — paving the way for the more granular settlements that have become the norm of late.

In ending the expectation that organizations provide reasonable security before and after settlements are finalized, the LabMD case had the practical impact of forcing the FTC to begin issuing more detailed complaints alleging how respondents violated federal law and to begin drafting settlements containing more specific remedial measures beyond the requirement that they be "reasonably designed" to protect consumer information. Instead, FTC settlements now generally feature specific technological means to this end.

Present and future

More specific orders

Lightyear, the first case after the LabMD ruling, immediately demonstrated the FTC's new approach. The FTC alleged Lightyear failed to provide adequate security through the implementation of low-cost and readily available measures to protect consumers' personal information. The FTC alleged this failure led to multiple occasions where hackers gained unauthorized access to an unsecured storage device housing the unencrypted personal data belonging to 12.5 million consumers. By negative inference, using the settlement as a guide, had the company performed routine vulnerability scanning, penetration testing, or other similar measures, Lightyear could likely have detected the attacks and protected consumers' personal information.

Although the complaint still alleged a failure to provide "reasonable security," the settlement included no such requirement to implement an information security program reasonably designed to protect consumer information. Instead, like every FTC settlement since Eli Lilly, Lightyear was required to implement and maintain a security program featuring technical, administrative, and physical safeguards, but the Lightyear settlement stipulated far more specific remedial actions which characterize the post-LabMD era.

One group of requirements for Lightyear is demonstrative — whereas previous settlements like BJ's required respondents to test and monitor the effectiveness of their information security program, the Lightyear settlement identified seven measures to execute the monitoring requirement, as indicated by the following chart:

BJ's	Lightyear
Test and monitor the effectiveness of the information security program.	Monitor all networks, systems, and assets to identify security events, including exfiltration.
	Restrict inbound IP connections; require authentication; limit access by function.
	Encrypt social security numbers and financial account information.
	Ensure secure installation and inventory of devices.
	Assess sufficiency at least once a year and promptly following any security incident.
	Test and monitor effectiveness at least once every 12 months.
	Perform vulnerability testing once every four months.

Specific technologies

Even more recent settlements have built on the Lightyear model to specify individual technical measures that respondents must implement. The 2022 case against CafePress, an online retailer, contained the first-ever requirement that a respondent implement multi-factor authentication using a secure third-party application as part of its mandatory information security programs. As recently as the 2021 Zoom settlement, cases required respondents to implement more secure user authentication methods "such as" MFA, but had never outright required this solution.

Context matters in the MFA requirement in CafePress, because the FTC has promoted it to businesses and consumers for nearly a decade. FTC-authored regulations require MFA as a baseline security standard in the recently updated Safeguards Rule of the Gramm-Leach Bliley Act, which applies to financial services.

> ***FTC-authored regulations require MFA as a baseline security standard in the recently updated Safeguards Rule of the Gramm-Leach Bliley Act, which applies to financial services.***

Such consistent guidance by the FTC is not unique to the MFA context.

Future required technologies?

We can infer from the MFA example in CafePress that the security technologies recommended by the commission today may be stipulated in future FTC enforcement actions. FTC resources like announcements, blog posts, policy statements, business guidance documents, and industry-specific regulations may provide clues as to which technologies those could be. Based on recent announcements, it may be reasonable to predict that privacy-enhancing technologies like deidentification technologies and encryption are likely contenders for remedies in future FTC settlements. This is particularly clear in the context of reproductive health products and services.

Likely involving sensitive health information

Protections for consumer-oriented health data not covered by the Health Insurance Portability and Accountability Act, the country's main health privacy regulating law, have drawn increasing focus from the FTC. In 2016, the FTC issued a set of best practices for mobile health developers, which encouraged them to use greater security and privacy controls like data minimization, deidentification, access permissions and limitations, authentication, including MFA, security by design, the use of software-development kits, and more.

In 2021, the commission issued a policy statement that clarified the Health Breach Notification Rule, which requires vendors that manage personal health records and related entities to notify consumers following a breach involving unsecured information, applies to most health apps and similar technologies. Also in 2021, Flo Health, which makes a popular fertility-tracking app, settled charges that it shared sensitive user data without user consent.

This summer, President Biden signed Executive Order Protecting Access to Reproductive Health Care Services in response to the Supreme Court's overturning of the right to an abortion. Part of the Executive Order directs the FTC to confront violative practices related to protecting consumers' privacy when seeking information about and provision of reproductive health services. In response, the FTC issued a statement that it considered location and health information, particularly regarding personal reproductive matters, to be among the most sensitive information deserving of enhanced privacy and security protections.

In its statement, the FTC said it was "committed to using the full scope of its legal authorities to protect consumers' privacy" and that it "will vigorously enforce the law if we uncover illegal conduct that exploits Americans' location, health, or other sensitive data. The FTC's past enforcement actions provide a roadmap for firms seeking to comply with the law," a nod to the utility of FTC common law in inferring baseline security standards.

And while past FTC cases are instructive in many circumstances, the statement points to one important consideration for companies processing consumer health records: "claims that data is "anonymous" or "has been anonymized" are often deceptive, adding that one set of researchers were able to (in some instances) uniquely identify 95% of a data set of 1.5 million individuals using four location

points with timestamps. Thus, it is reasonable to suspect that deidentifying methods may play a part in future FTC settlements involving patient health and location data.

PETs

Data anonymization is a notoriously difficult topic in privacy as it involves tradeoffs between privacy and data utility and the risk that datasets may be re-identified using auxiliary information. Nevertheless, the FTC's recent statements conveying its commitment in health and location matters should prompt organizations to ask whether their anonymization techniques are adequate in the evolving regulatory and technical environment. But its statement on health and location data does not elaborate on specific methods to achieve anonymization, leaving organizations without guidance as to which method they should use to mitigate risks in individual circumstance.

Privacy engineers can deploy different types of privacy-enhancing technologies to anonymize data and maintain user privacy while preserving data utility. There are many PETs that organizations could consider in implementing viable methods to satisfy the FTC's expectation that health and location information be protected. These include different approaches to pseudonymization, obfuscation, differential privacy, homomorphic encryption, and many more.

One possible source of guidance relates to fixed deidentification standards under the HIPAA regime, but criticisms of the fixed nature of HIPAA's requirements are part of the hotly-debated topic of anonymization and risk. Further, consumer-oriented health products and services are not covered by HIPAA, prompting the question of whether non-HIPAA-covered organizations are willing to implement HIPAA's fixed standards.

Therefore, it is crucial that companies within the scope of the FTC's statement on health and location evaluate which, if any, methods they use and whether those methods satisfy the commission's expectations regarding anonymization of both health records and location data.

Conclusion

In becoming more specific, recent FTC orders have changed the baseline security standards inferred from FTC common law. This naturally prompts organizations within the FTC's jurisdiction to ask whether they should internalize technical components identified in post-LabMD settlements to keep up with evolving FTC standards. Organizations that wish to stay ahead of the curve should look to security practices and technologies like PETs not currently required in any FTC settlements that could become featured in future ones by scrutinizing other FTC guidance. Non-HIPAA-covered health and location data is one important case study, but guidance documents point to other technical measures in other contexts. No catch-all answer exists to this question, but that should not stop organizations from evaluating current practices with an eye toward possible future FTC expectations.

Contact

Mark Thompson
Chief Strategy Officer, IAPP
mthompson@iapp.org

Cobun Zweifel-Keegan, CIPP/US, CIPM
Managing Director, Washington, D.C.
cobun@iapp.org

Samuel Adams*
Privacy Fellow, Future of Privacy Forum

IAPP Research and Insight
research@iapp.org

Müge Fazliglu, CIPP/E, CIPP/US
Senior Westin Research Fellow, IAPP
muge@iapp.org

Follow IAPP on Social Media

Published September, 2022.

**The work on this white paper was done solely in his previous capacity as Westin Fellow at the IAPP.*