



Breaking the Cycle: Addressing Underlying Causes of Systemic Data Risk
Remarks from the Chief Technologist Stephanie T. Nguyen
As Prepared for Delivery - Pittsburgh, Pennsylvania
The National Science Foundation's Secure and Trustworthy Cyberspace Principal Investigators'
Meeting (SaTC 2024) hosted by Carnegie Mellon University's CyLab Security and Privacy Institute

September 2024

I want to start by thanking the CMU and NSF organizers for inviting me, and for convening this excellent community. I'm Stephanie Nguyen, Chief Technologist and head of the Office of Technology at the Federal Trade Commission – today's remarks are my own views and not that of the Commission or any Commissioner.

The FTC's mission is to protect consumers against unfair and deceptive acts and practices and prevent unfair methods of competition. Put more simply, the agency exists to ensure that consumers, workers, and businesses don't get tricked, bullied, or coerced in the marketplace, and that marketplaces are competitive. The FTC's authority covers a broad range of issues and conduct in the economy, including companies' data practices.

Given how data breaches can impact consumers, it is crucial for law enforcers such as the FTC to be vigilant in addressing them and encouraging practices to prevent them. From the perspective of a consumer, data breaches can often unfold like this: An incident occurs, exploiting some extant vulnerability. There are some generic communications to consumers, invoking anxiety, confusion, or helplessness as officials investigate the primal cause. After some degree of damage has been done, articles covering the incident are littered with tips on what consumers should now do. Consumers are left with the cost and consequences with little insight into the current and recurrent risks in the future.

And with the backdrop of the commercial surveillance economy and advancements in technology like the rise of generative AI, companies may have more incentives to aggregate and amass vast amounts of data to power their models.¹ Attackers can leverage generative AI to scale

¹ <https://www.ftc.gov/news-events/events/2024/01/ftc-tech-summit>;
<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/data-models-quote-book-tech-summit-ai>;
<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive>

and automate their phishing attacks more efficiently² and potentially create more advanced malware to avoid detection.³

The Federal Trade Commission has an extensive track record with privacy and security,⁴ and has taken on nearly a hundred data security cases, including with Equifax,⁵ Blackbaud,⁶ Uber,⁷ Venmo,⁸ Zoom,⁹ Twitter,¹⁰ and Snap.¹¹

Over the years, some reports have highlighted that data breaches have risen over time¹² or have impacted more people.¹³ The trends are mixed.¹⁴ The harms can vary.¹⁵ The definition of "breach"¹⁶ and reporting requirements vary by organization and region¹⁷ differ by source and can change over time.¹⁸ Data breaches occur so often that some claim people have become desensitized and feel helpless,¹⁹ potentially due to factors like power asymmetries and navigating a complex system to seek future protection or redress.

² <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals>; <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/approaches-address-ai-enabled-voice-cloning>;

³ <https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/>

⁴ <https://www.ftc.gov/business-guidance/blog/2024/03/ftc-privacy-security-update-what-your-business-needs-know>

⁵ <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>

⁶ <https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-blackbaud-related-allegations-firms-security-failures-led-data-breach>

⁷ <https://www.ftc.gov/news-events/news/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security-claims>

⁸ <https://www.ftc.gov/news-events/news/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information-consumers-about-ability-transfer-funds>

⁹ <https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement>

¹⁰ <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>

¹¹ <https://www.ftc.gov/news-events/news/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were-false>

¹² <https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/>

¹³ <https://privacyrights.org/data-breaches>

¹⁴ https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

¹⁵ <https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf>

¹⁶ <https://www.naag.org/issues/consumer-protection/consumer-protection-101/privacy/data-breaches/>;

<https://www.foley.com/wp-content/uploads/2024/04/23.45248-Data-Breach-Chart-4.10.24.pdf>;

<https://www.steptoe.com/a/web/172961/SteptoeDataBreachNotificationChart.pdf>

¹⁷ <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>; <https://www.itgovernanceusa.com/data-breach-notification-laws>;

<https://iapp.org/resources/article/state-data-breach-notification-chart/>;

<https://iapp.org/resources/article/data-breach-notification-in-the-united-states-and-territories/>;

¹⁸ <https://www.fcc.gov/document/fcc-adopts-updated-data-breach-notification-rules-protect-consumers-0>;

<https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule>;

<https://www.legis.state.pa.us/cfdocs/legis/li/uconsCheck.cfm?yr=2024&sessInd=0&act=33>;

<https://www.sec.gov/newsroom/press-releases/2023-139>; <https://www.sec.gov/newsroom/press-releases/2023-139>

¹⁹ https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf;

https://www.ftc.gov/system/files/documents/public_events/1582978/now_im_a_bit_angry_-_individuals_awareness_perception_and_responses_to_data.pdf

As the FTC Chair has noted before,²⁰ data and security vulnerabilities can have sweeping effects on the economy and on millions of consumers – which can damage and disrupt critical systems including hospitals,²¹ food supply chains,²² transportation systems,²³ and financial services.²⁴ And far too often, the default action item veers toward: "What should *consumers* do about it?" While potentially helpful for some, this broad sentiment can codify an expectation that it is on the *consumers* to figure out how to use lifetime identity monitoring – or to educate and train themselves on how to navigate the latest threats.

At the FTC, our mission is to enforce the laws and protect consumers and competition. And technologists at the agency work to ensure we do not accept the status quo of harms to millions of people caused by unlawful behavior.

First, I'd like to state some grounding beliefs. I believe that information can empower people to make decisions. At the same time, information can inundate consumers²⁵ and obfuscate other critical information.²⁶

I believe in technology – and that it should work the way people expect that things should work. A flashlight app should allow you to use your phone's bright light – and not transmit your granular mobile device data to ad networks.²⁷ Consumers should be able to shop online without fear of review suppression or actors gaming the system.²⁸ People should be able to walk into a pharmacy without having a faulty facial recognition system unfairly target consumers as a shoplifter.²⁹

And I believe the burden should not primarily fall on consumers to shoulder navigating a complex system of data breaches and fend for themselves after damage has been done. Additionally, the market should not be left alone to "self-regulate."³⁰ At the Office of Technology, our experts take the following approach:

Reject harms as the status quo. First, while recognizing that technical challenges occur, it is critical to reject a status quo that accepts frequent and widespread data breaches as the norm.

20

https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf

²¹ <https://www.cnn.com/2024/05/10/tech/cyberattack-ascension-ambulances-hospitals/index.html>

²² <https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs>

²³ <https://www.seattletimes.com/seattle-news/transportation/cyberattack-shuts-down-wa-transportation-website-causing-havoc-for-ferry-passengers-others/>

²⁴ <https://www.cNBC.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html>

²⁵ [Information Overload | Pew Research Center](#)

²⁶ [Distracted: The New News World and the Fate of Attention - Nieman Foundation \(harvard.edu\)](#)

²⁷ <https://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf>

²⁸ <https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials>

²⁹ https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf

³⁰ https://www.ftc.gov/system/files/ftc_gov/pdf/remarks-of-samuel-levine-at-nad-2023.pdf;

https://www.ftc.gov/system/files/ftc_gov/pdf/samuel-levine-remarks-for-ot-ai-summit.pdf;

<https://www.ftc.gov/news-events/news/speeches/remarks-chief-technologist-stephanie-t-nguyen-prepared-delivery-association-computing-machinery-acm>;

This is akin to how FTC is taking "bold steps to move away from the flawed, [failed,³¹ and broken]³² 'notice and choice' privacy framework."³³ "While the state of the art in software continues to improve, there are known approaches that systemically and preemptively address many potential issues, either entirely preventing them or dramatically reducing the likelihood of them occurring," FTC staff shared.³⁴

Scrutinize business model incentives. Second, we must focus on how business models drive incentives, and vice versa.³⁵ We recognize that the proximal causes of data breaches are varied. They can stem from shifts in technology capabilities and markets, shifts in reporting requirements, bad actors and ransomware attacks,³⁶ or just bad company practices.³⁷ The rise of commercial surveillance³⁸ has been underscored by social media platforms powered by advertising,³⁹ personalization and recommendation systems,⁴⁰ data brokers,⁴¹ new forms of pixel tracking,⁴² and generative AI powered technology which relies on a large amount of data as its core foundation.⁴³ Incumbent companies can continue to amass more data, which can continue to fuel consolidation in the market.⁴⁴

Address underlying causes of risk. With technologists working with attorneys on enforcement and investigations, it is essential to continue to strengthen remedies by addressing underlying causes of risk in complex systems.⁴⁵ "This means focusing on structural incentives that enable conduct – [like] conflicts of interest, business models, or structural dominance – as well as looking upstream at the firms that are enabling and profiting from this conduct," Chair Khan

³¹ https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf

³² https://www.ftc.gov/system/files/ftc_gov/pdf/stephanie-nguyen-remarks-facct-june-2024_0.pdf

³³ https://www.ftc.gov/system/files/ftc_gov/pdf/testimony-chair-khan.pdf

³⁴ <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/08/avoiding-outages-preventing-widespread-system-failures>

³⁵ https://www.ftc.gov/system/files/ftc_gov/pdf/2024.01.25-chair-khan-remarks-at-ot-tech-summit.pdf

³⁶ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a>

³⁷ https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf

³⁸ <https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html>;

<https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>;

³⁹ [Social Media Companies Collect So Much Data Even They Can't Remember All The Ways They Surveil Us \(forbes.com\)](https://www.forbes.com)

⁴⁰ [AI's golden rule: Good data inputs equal better AI outputs - Fast Company](https://www.fastcompany.com)

⁴¹ <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket>;

<https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

⁴² <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>

⁴³ <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns>

⁴⁴ <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns>

⁴⁵ I'd like to note that this has always been a goal of FTC data breach orders

<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

shared.⁴⁶ This also means "securing meaningful remedies to protect consumers' information, rather than placing the burden on consumers to protect themselves," said Bureau of Consumer Protection Director Sam Levine.⁴⁷ The FTC has incorporated policies and procedures to address underlying causes of risk⁴⁸ due to over collection, storage, and retention of data - like multi-factor authentication⁴⁹ and requiring that a company's systems are encrypted and authenticated.⁵⁰

In addition to these practices, the FTC aims to address more upstream harms include:

1. Minimizing data collection⁵¹ and establishing data retention policies. The agency has secured orders prohibiting indefinite retention and requiring the implementation of data retention schedules,⁵² including one limited to the "shortest time necessary"⁵³ to fulfill the original purpose of the data collection.

⁴⁶https://www.ftc.gov/system/files/documents/public_statements/1596664/agency_priorities_memo_from_chair_lina_m_khan_9-22-21.pdf

⁴⁷ <https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update>

⁴⁸ <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>

⁴⁹ The Cafepress order references examples of secure authentication protocols to include cryptographic software or devices, mobile authenticator applications, or allowing the use of security keys;

https://www.ftc.gov/system/files/ftc_gov/pdf/192%203209%20-%20CafePress%20combined%20package%20without%20signatures.pdf

⁵⁰ Twitter: <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023062-twitter-inc-us-v;>

Chegg: <https://www.ftc.gov/legal-library/browse/cases-proceedings/cheegg>; Drizly: <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter>; CafePress: <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter>;

Global Tel*Link: <https://www.ftc.gov/legal-library/browse/cases-proceedings/2123012-global-tel-link-corporation>

⁵¹ https://www.ftc.gov/system/files/documents/public_statements/1592854/slaughter_statement_privacycon_7-27-21.pdf;

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

⁵² Alexa: <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v;>

Cafepress: https://www.ftc.gov/system/files/ftc_gov/pdf/1923209CafePressComplaint.pdf

Blackbaud: <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023181-blackbaud-inc>

Education Technology & COPPA Policy Statement:

https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf

Drizly: <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>

Chegg: <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-cheegg-careless-security-exposed-personal-data-millions>

BetterHelp: <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>

Premom: <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

Global Tel*Link: <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-finalizes-order-global-tellink-over-security-failures-led-breach-sensitive-data>

X-Mode/Outlogic: <https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data>

Alexa: <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>

⁵³ Cerebral: <https://www.ftc.gov/legal-library/browse/cases-proceedings/222-3087-cerebral-inc-kyle-robertson-us-v>

2. Creating bright line limits on sensitive uses of data. The FTC has recognized that sensitive data including location,⁵⁴ browsing,⁵⁵ kids, health and financial data requires strengthened protections.⁵⁶ So the FTC has obtained orders in cases that restrict data use and sharing, including with third-parties,⁵⁷ including for advertising purposes.⁵⁸

3. Enacting data and model deletion. Unlawful data collection can bring considerable benefits to companies which presents a challenge to deter such abuses and prevent violations going forward. For example, firms can train their models on illegally obtained data.⁵⁹ This is why the agency has required companies to not only destroy data they collected illegally but also destroy the models trained on that data.

Finally, a key part of our role is the ability to communicate our work, learn from subject matter experts, and translate some of the agency's findings to communities who can help amplify the FTC's mission. There are practical insights and learnings the FTC can offer to the research community in the form of our legal complaints and legal orders which can be useful tools to better understand what type of evidence is helpful to bring cases and what the FTC can do about it.

As we navigate the sessions today: How can we better connect our research to acknowledge and scrutinize business incentives? How can our work address underlying causes of risk? How can researchers and practitioners best engage on upstream remedies? These are the questions we'll discuss in our afternoon roundtable. As we continue to live and participate in the digital economy, we must remain vigilant about the risks that come with it. We must act and translate our research into practice. We are at a crossroads with a massive shift in technology where the status quos we do – or don't – accept and the choices we make about protecting consumers will shape our future. We hope to see many of you this afternoon. Thank you.

I'd like to thank my colleagues, Amritha Jayanti, Simon Fondrie-Teitler, Sam Levine, Leah Frazier, Jess Weiner, Bikram Bandy for your contributions to the agency on this topic, your insights and support in reviewing these remarks.

⁵⁴ <https://www.ftc.gov/legal-library/browse/cases-proceedings/2123038-x-mode-social-inc>

⁵⁵ <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023033-avast>

⁵⁶ <https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>

⁵⁷ 1Health / Vitagene: <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-says-genetic-testing-company-1health-failed-protect-privacy-security-dna-data-unfairly-changed>

FloHealth: <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

⁵⁸ BetterHelp: <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>

Premom: <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

⁵⁹ <https://www.ftc.gov/news-events/news/press-releases/2023/11/InCommentSubmittedtoUSCopyrightOfficeFTCRaisesAIrelatedCompetitionandConsumerProtectionIssuesStressingThatItWillUseItsAuthoritytoProtectCompetitionandConsumersinAIMarkets>