UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Melissa Holyoak

Concurring Statement of Commissioner Melissa Holyoak

Verkada, Inc., FTC Matter No. 2123068

August 30, 2024

I support the Commission's settlement with building security company Verkada, Inc., whose allegedly unreasonable data security practices led to unauthorized access of its customers' cameras, including cameras placed in sensitive locations, such as elementary schools, psychiatric hospitals, and women's health clinics. The complaint also alleges that Verkada deceived consumers in other ways, including with online reviews written by its employees and a venture capital investor. And, according to the complaint, Verkada's mass email marketing campaigns to small businesses violated the CAN-SPAM Act. I write separately with a few words of caution about prescribing the specific manner in which businesses safeguard consumers' personal information.

For many years, the Commission's orders in data security matters have required the respondent or defendant to implement a comprehensive data security program that is periodically reviewed by an independent third-party assessor whose findings the Commission can review. I support this approach, which requires companies under FTC orders to have reasonable security,[1] which usefully leverages external expertise to supplement the Commission's, and whose safeguards promote order enforceability.[2]

Over the past few years, however, the data security programs in the Commission's settlements have become ever more prescriptive, mandating particular controls, such as multi-factor authentication.[3] At first blush, prescribing particular security controls for a company that has allegedly failed to safeguard consumers' data appears prudent. But these are not requirements of short duration; over the twenty years during which the data security program is required, such specific prescriptions may become dated as technology and threats evolve.

---

[1] The Commission has long said that Section 5 of the FTC requires *reasonable* security, not perfect security. Not every breach entails a Section 5 violation, as Section 5 does not impose strict liability on data holders. *See, e.g.*, Federal Trade Commission, Statement Marking the FTC's 50th Data Security Settlement, at 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf ("Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.").

[2] Andrew Smith, New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers, FTC Business Blog, Jan. 6., 2020, https://www.ftc.gov/business-guidance/blog/2020/01/new-and-improved-ftc-data-security-orders-better-guidance-companies-better-protection-consumers.

[3] *See, e.g.*, Agreement Containing Consent Order, *Residual Pumpkin*, FTC No. 1923209, at 4 (Mar. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Residual%20Pumpkin%20Agreement%20Containing%20Consent%20Order.pdf (requiring "[r]eplacing authentication measures based on the use of security questions and answers to access accounts with multi-factor authentication methods that use a secure authentication protocol, such as cryptographic software or devices, mobile authenticator applications, or allowing the use of security keys").

Mandating rigid controls that do not scale with size, sensitivity, or evolving threats will undercut the Commission's goal of reasonable data security while burdening businesses in a manner that is likely to raise costs for consumers. And requiring such controls for *twenty years* may be disproportionate to the misconduct alleged in many data security orders—and far more likely to raise transaction costs between firms and consumers (and to spawn a cottage industry of FTC order assessors) than to facilitate efficient investments in data security.[4]

I strongly support the Commission's work to protect the security of consumers' personal information. But that work must be grounded in legal requirements, such as Section 5's requirement of reasonable security.[5] To that end, as the Commission addresses data security in enforcement actions and evaluates public comments about data security received in response to the Advance Notice of Proposed Rulemaking Regarding Commercial Surveillance and Data Security,[6] the Commission should promote a flexible, risk-based approach to data security that creates incentives for efficient investment in data security. Hewing to the law in this manner will benefit consumers, businesses, and this institution alike.

[4] Importantly, the multi-factor authentication requirement in this order contains an "escape valve," that allows the company to use a different authentication method where the company properly justifies and documents the reason for doing so. Stipulated Order at 9.

[5] The Commission enforces other laws related to data security, such as the Safeguards Rule, 16 C.F.R. pt. 314, and the COPPA Rule, 16 C.F.R. pt. 312.

[6] 87 Fed. Reg. 51273 (Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.