Updates
January 11, 2023

Four Data Security Safeguards the FTC Would Like Companies To Adopt in 2023

Data security will undoubtedly remain an enforcement priority for the Federal Trade Commission in 2023. A presentation on the FTC's approach to data security by Deputy Chief Technologist Alex Gaynor at a Commission open meeting on December 14, 2022, highlighted four provisions found in one or more recent FTC consent orders as particularly important, though not reflecting the full array of safeguards the FTC expects organizations to employ. For businesses looking to shore up their cybersecurity measures in 2023, these four practices are worth considering:

- **"Enhanced" multifactor authentication (MFA) for users.** Gaynor described the adoption of MFA as a "fantastic" addition as a security measure because it gives users tools to protect themselves by helping to ensure that their accounts cannot be compromised solely through access to their passwords. However, he explained that recent FTC orders have gone beyond merely requiring MFA. For example, at least one order specifically required a company to replace legacy authentication practices, such as security questions, which Gaynor suggested were problematic because they require consumers to provide more personal information, which is often publicly available to would-be attackers. Gaynor also noted that some recent orders specify that information collected via MFA may be used for authentication purposes only.
- **Phishing-resistant MFA for personnel.** Recent FTC orders have also required that companies use "phishing-resistant" MFA for their personnel to access corporate networks. According to Gaynor, most forms of MFA do not fully protect against phishing because if users can be tricked into typing in their passwords, they can be tricked into typing in a code from their phone. Gaynor expressed the view that physical security keys and passkeys are a stronger form of MFA because physical possession of the key (i.e., by the authorized user) is needed for successful authentication. Gaynor describes physical security keys and passkeys as "revolutionary."
- **Encrypting and authenticating all connections ("zero trust").** According to Gaynor, the prior state of the art in data security focused on strong firewalls to prevent unauthorized access to corporate networks. Yet, they did little to prevent attackers from moving freely once inside, such that an attacker who found a vulnerability, however small, could obtain the "keys to the kingdom." In recent orders, the FTC has sought to require that users be authenticated *and* authorized to access systems within the network and that connections be encrypted to prevent attackers from snooping on legitimate connections (i.e., those built on the principle of "zero trust"). Gaynor said these practices "dramatically limit the blast radius of a vulnerability," providing systems inside a corporate network the same amount of protection that companies provide to the initial points of entry.
- **Data minimization.** Finally, recent orders require companies to establish, publish, and follow a data retention schedule. According to Gaynor, a data retention schedule requires a company to have a strong internal catalog of all data stored, helps ensure that companies can comply with data deletion requests, and provides companies with the information needed to prioritize protections based on the types and sensitivities of data they store.

These order provisions, and the practices they require, reflect the FTC's emphasis on a systemic approach to data security that anticipates and designs for human error. In particular, Gaynor urged companies to consider how a system's design can cause or facilitate human error—to consider, for example, "did the system make it easy for a human to make a mistake?"; "was the human warned about the risks of what they were doing?"; and "was the

human warned, but in fact, these warnings show up so often (even in completely safe situations) as to numb them to the warnings?"

FTC Chair Lina Khan added that beyond the systemic approach reflected in Gaynor's presentation, the FTC is also focusing on accountability and administrability of its data security orders. Additional measures include holding corporate officers personally liable in some orders so that inadequate security practices are not viewed as a cost of doing business and including order language that facilitates the FTC's ability to effectively oversee and enforce its orders.

Takeaway

FTC consent orders impose requirements only on those subject to the orders, not on all industry. But consent orders are a good place to learn what compliance measures the FTC believes businesses should adopt. So, companies looking to put themselves in the FTC's good graces as we enter 2023 would do well to consider if they can implement or shore up these four measures.

Authors

Janis Kestenbaum

Partner
JKestenbaum@perkinscoie.com

Rebecca S. Engrav

Partner
REngrav@perkinscoie.com 206.359.6168

Aaron Haberman

Counsel
AHaberman@perkinscoie.com 202.654.6246

Emma Roberts

Associate
EmmaRoberts@perkinscoie.com 469.801.2305

Explore more in

Privacy & Security Communications Digital Media & Entertainment, Gaming & Sports Retail & Consumer Products

Related insights

Update

OFCCP Set To Release Contractors' EEO-1 Reports to FOIA Requestors

Update

Securities Enforcement Forum DC 2024: Priorities in the Election’s Wake