LAW360®

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC Actions Highlight Focus On Cos.' Cybersecurity Efficacy

By **Stephenie Gosnell Handler, Svetlana Gans and Kunal Kanodia**
(January 4, 2023, 2:42 PM EST)

Stephenie Gosnell Handler

Svetlana Gans

Kunal Kanodia

On Dec. 14, the Federal Trade Commission hosted an open meeting featuring a staff presentation on cybersecurity.

Alex Gaynor, the FTC's deputy chief technology officer, discussed the implications of the FTC's approach to data security enforcement over the past year, specifically highlighting four security best practices.

He noted that the FTC's latest orders signaled an important new focus on addressing flaws in the nuts and bolts of companies' cyber programs that leave user and employee data vulnerable in an increasingly digital economy.

The presentation gives important context by reviewing the FTC's enforcement actions over the course of 2022[1] and in light of broader federal government trendlines as stipulated in President Joe Biden's Executive Order No. 14028 on improving the nation's cybersecurity.[2]

This review indicates the FTC is exerting heightened focus on assessing certain technical security safeguards, the absence of which can create exploitable gaps that undermine appropriate management of data.

The FTC's emphasis on certain core technical measures is instructive for all companies, regardless of size or industry, in order to minimize cyber risk and regulatory scrutiny.

FTC Presentation Shows Clear Approach to Security Best Practices

Gaynor contextualized the FTC's approach to data security enforcement over the past year, which he said was focused on addressing the true causes of data security risks.

He noted the FTC's new approach reflects the importance of using modern technologies to address costs relating to data security, and identified two books — "Behind Human Error"[3] by Leila Johannesen, Richard Cook, David D. Woods, Nadine Sarter and Sidney Dekker, and "Engineering a Safer World"[4] by Nancy Leveson — that formed the basis of his thinking.

One of the authors of "Behind Human Error," Cook, emphasized that human error should only be the beginning — and not the end — of an investigation. Instead, focus must be placed on raising questions about whether this error was easily caused by the system.

The FTC's latest approach seems to accept this thesis, as it increasingly focuses on systemic inadequacies that allowed system vulnerabilities in the first place, as opposed to individual errors.

The FTC's data security orders send a signal to the market as to what constitutes reasonable protections of user data.

This is evidenced in the FTC's October settlement with Chegg Inc.,[5] which penalized Chegg for alleged lax internal security protocols, such as storing personal information on cloud databases in plain text and without encryption, the lack of any policy regarding deleting user information that was no longer necessary, and its alleged failure to prevent multiple successful phishing attacks that led to the leak of customers' and employees' personally identifiable information.[6]

Similarly, the FTC made it clear in October that it viewed Drizly LLC's innate system vulnerabilities as a proximate cause of the breach of 2.5 million customers' data.[7]

And, the FTC's March settlement with CafePress Inc.[8] regarding its security program that allegedly led to the exposure of more than 180,000 unencrypted Social Security numbers[9] emphasized that companies must minimize the amount of data they collect and retain.

Finally, the FTC's January settlement with Everalbum Inc.,[10] where the company allegedly did not comply with user requests to delete accounts or biometric data, indicates that companies must also respect user requests to delete data, or provide consent for the company to keep that data.

FTC's Recommendations to Minimize System Vulnerabilities

Gaynor's ultimate recommendations are fourfold. In our experience, these recommendations generally track evolving industry best practices and are also aligned with diverse regulator guidance and expectations.

Use multifactor authentication.

First, companies should implement multifactor authentication[11] for users. Gaynor noted that this is a critical security practice that gives users a key tool to protect themselves.

Legacy practices like security questions are not as effective as multifactor authentication, because such practices often require that the user provide even more personal information to companies than users typically would.

Further, it might be easy for an attacker to look up this information or otherwise accurately guess personal information.

The FTC's focus on multifactor authentication is clear: The Chegg, Drizly, and CafePress decisions all require the relevant companies to provide multifactor authentication as an option for consumers.[12]

Ensure that a phishing-resistant form of multifactor authentication is used by employees.

Second, Gaynor added that companies should have personnel use multifactor authentication that specifically provides adequate protection against phishing.

This goes beyond the traditional user education against phishing attacks, and places increased onus on the system rather than the user for preventing successful phishing attacks.

Importantly, this recommendation is distinct from multifactor authentications that rely on app-based authentication — one-time password, mobile push notifications or token-based, one-time passwords — or SMS multifactor authentication, given the probability of users being tricked into typing additional codes.

Rather, Gayor emphasized that companies should use secure authentication protocols such as cryptographic software or mobile authenticator applications that ensure that users trying to access their accounts are physically present where they are trying to access their accounts,[13] rather than relying on a code that is not tied to a geographic location or physical presence.

This is consistent with U.S. Cybersecurity and Infrastructure Security Agency recommendations issued in October,[14] and is also required under the Chegg, Drizly and CafePress orders.[15]

These orders require that the companies not include telephone or SMS-based authentication methods, but use options that are resistant to phishing attacks.

Encrypt and authenticate all connections within company system.

Third, Gaynor suggested that companies should implement a zero-trust architecture system that requires encryption and authentication of all connections within company systems, rather than granting global access to any individual who manages to get access within the network.

This may require a significant shift in security strategy, as many organizations still focus on perimeter defense — such that if the outer perimeter, e.g., system firewall, is compromised, attackers are able to move laterally within the network, which can result in the attackers escalating privileges and achieving malicious goals of compromising sensitive systems and exfiltrating data.

In contrast, zero trust is a collection of concepts and principles that assumes compromise and requires continuous validation at every stage of interaction, e.g., not just the perimeter.

This is a significant strategic and cultural shift from location-centric security models to a more data-centric approach.[16]

The National Security Agency's guidance on zero-trust architecture is instructive here.

Federal agencies are required to assume that a breach is inevitable, thus they would need to limit access to only what is needed, and embed comprehensive security monitoring, risk-based access controls and system security automation.[17]

Biden's executive order[18] requires federal agencies to take action to develop zero trust architecture, although this requirement does not currently extend to the private sector.

Yet Gaynor indicated that zero-trust should be the go-forward security strategy, requiring authentication and encryption at all stages, and building on strong identities against phishing and multifactor authentication.

The recommendation to focus on zero-trust architecture could be seen as an example of an access control mechanism, which the FTC has long required as part of its risk-based cybersecurity safeguards in its orders.

However, the increased focus on zero-trust architecture — which can require a significant re-architecting and investment to implement — signals that the FTC will increasingly expect more sophisticated approaches for this technical safeguard.

While we have not yet seen mention of zero-trust architecture per se in FTC orders, the evolving standard was most recently reflected in its Chegg order, where the FTC required Chegg to implement data access controls for all assets, restrict inbound and outbound connections, keep records of network access to track anomalous activity and active threats, and limit employee access only to what is needed to perform that employee's job function.[19]

Comply with data retention schedules.

Finally, Gaynor discussed the need for companies to create and adhere to detailed and precise data retention schedules.

He noted that these data retention schedules should require a strong internal catalog of all data stored by the company that would assist in compliance with requests from users to delete their data. This also allows companies to focus on data that needs the most protection.

But Gaynor also added that the most secure data is"data that's not stored at all — indicating that companies should also focus on data minimization, as noted in both the Chegg and Drizly orders.[20]

Data minimization is the principle that system controls should ensure adequate and consistent removal of unnecessary data: businesses should only retain data for a specified business need and comply with set timeframe for deletion.

The emphasis on this principle was seen in the FTC's advanced notice of proposed rulemaking that rolled the concept of data minimization into the definition of data security.[21]

And, in the Chegg, Drizly and CafePress decisions, the FTC ordered the companies to destroy data not used in connection with providing products to businesses, and prevent the collection of such data in the future.[22]

These controls suggest that the FTC wants businesses to retain data only where there is a specific business need for it, and continue to adequately and consistently remove data even after it is collected.

Especially where companies store personal data that is not used to provide products or services, that personal data should not be collected in the first place.[23]

Finally, as evinced by the Everalbum order, companies are expected to delete data in compliance with consumer requests and in compliance with applicable statutes, such as biometric data statutes.[24]

Conclusion

Taken together, this presentation puts the FTC's recent Chegg, Drizly, CafePress and Everalbum orders in context, and indicates a larger shift in focus to efficacy of companies' system controls in dealing with user data.

The four priority areas of focus span a range from well-supported best practices, such as the use of multifactor authentication, to evolving areas of best practice like zero trust that may take dedicated strategic shifts to implement.

All four areas reinforce the FTC's particular focus on how companies protect and manage user data through the technical safeguards on their systems and networks.

The push toward data minimization — as we saw in the Chegg and Drizly orders this year — means that companies should continue to be intentional about the amount of data they retain control over after the purpose for which it was collected has ceased to exist.

This reflects the FTC's underlying concern that users are adequately protected and their requests for data deletion are complied with.

As we look forward to 2023, companies should consider how these four recommendations align with their own cybersecurity strategy and risk management approach, and prioritize as appropriate.

Stephenie Gosnell Handler is a partner at Gibson Dunn & Crutcher LLP.

Svetlana S. Gans is a partner at the firm. She previously served as chief of staff to Maureen K. Ohlhausen, former FTC acting chairman.

Kunal Kanodia is an associate at the firm.

Law clerk Apratim Vidyarthi contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Decision and Order, In the Matter of Chegg, Inc., F.T.C. File No. 2023151, (Oct. 31, 2022) (consent order), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Decision-and-Order.pdf (mandating improved cybersecurity requirements, limitations on data collection and retention, multifactor authentication, and allowing users access to and deletion of their data) (hereinafter Chegg Decision and Order); Decision and Order, In the Matter of Drizly, LLC, F.T.C. File No. 2023185 (Oct. 24, 2022) (consent order), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf (mandating cybersecurity program, destruction of unnecessary data, restricting future data collection and retention, and binding CEO individually to specific cybersecurity requirements) (hereinafter Drizly Decision and Order); Decision and Order, In the Matter of CafePress, FTC Docket No. C-4768 (June 24, 2022) (consent order), https://www.ftc.gov/system/files/ftc_gov/pdf/192%203209%20-

%20CafePress%20combined%20package%20without%20signatures.pdf (mandating cybersecurity program including inter alia encryption, multifactor authentication, and data minimization) (hereinafter CafePress Decision and Order); Decision and Order, In the Matter of Everalbum, Inc., F.T.C. File No. 1923172, (May 6, 2021) (consent order), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf (mandating notice and consent requirements, deletion of deactivated account user data, recordkeeping, and compliance and monitoring of deletion program) (hereinafter Everalbum Decision and Order).

[2] Exec. Order No. 14,028, 86 Fed. Reg 26,633 (May 12, 2021).

[3] David D. Woods et al., Behind Human Error (2d ed. 2010).

[4] Nancy G. Levinson, Engineering a Safer World (2016).

[5] Chegg Decision and Order.

[6] Complaint, In the Matter of Chegg, Inc., F.T.C. File No. 202-3151 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf.

[7] Complaint, In the Matter of Drizly, LLC, F.T.C. File No. 2023185 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf.

[8] CafePress Decision and Order.

[9] Complaint, In the Matter of CafePress, F.T.C. No. 1923209 (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/CafePress-Complaint_0.pdf.

[10] Everalbum Decision and Order.

[11] Multi-factor authentication is defined as "s a layered approach to securing physical and logical access where a system requires a user to present a combination of two or more different authenticators to verify a user's identity for login."

Fact Sheet, Cybersecurity & Infrastructure Security Agency (January 2022), https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf.

[12] Chegg Decision and Order; Drizly Decision and Order; CafePress Decision and Order.

[13] Implementing Phishing-Resistant MFA, Cybersecurity & Infrastructure Security Agency (Oct. 2022), https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[14] https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[15] Chegg Decision and Order; Drizly Decision and Order; CafePress Decision and Order.

[16] See CISA Zero Trust Maturity Model (Pre-Decision Draft), Cybersecurity & Infrastructure Security Agency (June

2021), https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[17] Embracing a Zero Trust Security Model, NATIONAL SECURITY AGENCY (Feb. 2021) https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[18] Exec. Order No. 14,028, 86 Fed. Reg 26,633 (May 12, 2021).

[19] Chegg Decision and Order.

[20] Chegg Decision and Order; Drizly Decision and Order.

[21] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg 51,273 (Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[22] Chegg Decision and Order; Drizly Decision and Order; CafePress Decision and Order.

[23] Id.

[24] Everalbum Decision and Order.