Skadden

Privacy & Cybersecurity Update

FTC Chair Suggests Changing Approach to Data Privacy and Security Regulation

Federal Trade Commission (FTC) Chairperson Lina Khan has suggested that the commission consider rethinking its traditional "notice and consent" approach to privacy regulation in the United States.

On April 11, 2022, Ms. Khan spoke at the International Association of Privacy Professionals' Global Privacy Summit in Washington, D.C. and stated her position that the FTC is well suited to tackle and appropriately police the new political economy of how companies collect and deploy data in America.

Background

Ms. Khan was appointed as chair of the FTC in June 2021, and although her focus prior to assuming her role had been on antitrust and competition, Ms. Khan has made it clear that she anticipates making changes in the privacy sector. The FTC currently faces a 2-2 partisan deadlock, however commissioner nominee Alvaro Bedoya is expected to be confirmed to the FTC in the coming weeks. Mr. Bedoya's confirmation as an FTC commissioner will therefore provide Ms. Khan with the majority she would need to steer the FTC in a new direction.

Using its specific authority under the Gramm-Leach-Bliley Act (among other laws) and its general authority under the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce," the commission has been the primary regulator of privacy and data security practices in the U.S. for decades. It has exercised its authority in a variety of ways, but has often followed a "notice and consent" framework that compares what companies disclose in their privacy policies with their actual practices.

Ms. Khan's Remarks

The Shifting Data Landscape and Power Inequities

Ms. Khan's remarks at the IAPP Global Privacy Summit outlined the existing privacy landscape and the shift seen over the last few years regarding the digitization of the economy, particularly due to the pandemic. Ms. Khan's statements throughout her address considered the benefits and risks of digitization and how the FTC plans to undertake the challenge of effectively policing and remedying data and security issues.

She stated at the summit that "(t)he general lack of legal limits on what types of information can be monetized has yielded a booming economy built around the buying and selling of this data." [1] Ms. Khan also expressed her belief that the data practices of today create and exacerbate "deep asymmetries of information," further worsening the inequalities of power between businesses and consumers. Additionally, she said the FTC is focusing on adopting an approach to address and rectify unlawful data practices, while focusing on three key aspects:

- employing the FTC's limited resources to maximize impact, predominantly focusing on firms whose business practices cause widespread harm to consumers;
- using an interdisciplinary approach by evaluating data practices through both a consumer protection and competition lens; and
- focusing on implementing effective remedies when faced with violations of the law.

Notice and Consent Model May Be Inadequate; Substantive Limits on Data Gathering May Be Appropriate

In her remarks, Ms. Khan indicated that the FTC may need to change its approach to protecting consumers. Specifically, she indicated that the commission also needs to "reassess the frameworks it presently uses to assess unlawful conduct" and that "the present market realities may render the present notice and present paradigm outdated and insufficient" for consumers to understand businesses' data collection practices. She suggested that the existing notice and consent paradigm causes companies and policymakers to focus on "process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place."

As an alternative to the traditional notice and consent approach, Ms. Khan suggested that the FTC may need to explore "substantive limits" on data practices rather than focus on procedural protections for consumers. She indicated that the FTC is "considering initiating a rulemaking to address commercial surveillance and lax data security practices" and called for privacy legislation from Congress, which she stated would "help usher in this type of new paradigm."

State and Federal Privacy Laws

As the FTC debates a future direction regarding privacy, many states are passing their own privacy-related legislation with robust requirements for businesses regarding data collection practices and consumer protection. To date, California, Colorado, Virginia and Utah have passed comprehensive data privacy laws, with many other states considering passing their own similar legislation. This trend is likely to continue; the more states that pass data privacy laws, the more other states will feel pressure to do so.

At the same time, Congress continues to work on a comprehensive federal privacy law, but many open issues remain, including whether such a law would override state laws, as well as whether individuals should have a right to sue businesses over how their data is handled.

Key Takeaways

Ms. Khan's remarks suggest that the FTC, following the confirmation of Mr. Bedoya, may dramatically shift its approach to privacy regulation in the U.S. While it remains to be seen what direction the FTC might take — especially given the possibility of new federal laws in this area — a significant shift in the FTC's approach could have a dramatic impact on certain types of business practices.

Return to Table of Contents

European Data Protection Board Invites Feedback in Response to Draft Guidelines on Dark Patterns

The European Data Protection Board (EDPB) has published a draft set of guidelines on identifying and avoiding dark patterns on social media platforms.

On March 21, 2022, the EDPB published its draft guidelines on identifying and avoiding dark patterns in social media platform interfaces.[2] In the context of data protection, the term "dark patterns" (also known as "deceptive design") generally refers to the set of features implemented on social media platforms that can lead to confusion about how personal data is processed by the platform, which generally discourages users from exercising their rights as data subjects. The EDPB defines dark patterns as "interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data" and sets out 15 types of dark patterns, which are then split into six additional dark pattern categories. The guidelines are now open to a six-week period of consultation that ends on May 2, 2022, after which the EDPB will adopt a final version.

[1] Ms. Khan's full remarks are available here.

[2] The draft Guidelines are available here.

Background and Scope

The EDPB is the EU body responsible for the consistent application and implementation of the General Data Protection Regulation (GDPR) across the EU and is made up of the head of each member state's data protection agency (DPA) and the European Data Protection Supervisor. The EDPB's objective in publishing the guidelines is to provide designers and users of social media platforms with the information they need to identify and avoid these dark patterns (and, for those providing the platforms, to ensure they are not implementing practices that violate the GDPR). Whilst not legally binding, the guidelines link examples of dark patterns to provisions of the GDPR that they contravene, and therefore provide a useful indication of how the DPAs of the EU will enforce the GDPR.

The guidelines form part of the EDPB Strategy and Work Programme 2021-2023 (the strategy). Published in December 2020, the strategy sets out four pillars in its plan to further its overarching goals to ensure consistent application of the GDPR and promote effective cooperation amongst DPAs. The four pillars are: (1) advancing harmonization and facilitating compliance; (2) supporting effective enforcement and efficient cooperation between national DPAs; (3) a fundamental rights approach to new technologies; and (4) the global dimension (improving engagement with international bodies). Some of the key actions under the first pillar, for example, prompt the EDPB to provide guidance on key notions of data protection law and to raise awareness of data protection law for a wider audience, including amongst data subjects. Since the strategy was published, the EDPB has issued almost 20 sets of guidelines on topics such as the data subject's right of access and the virtual voice assistants.

Categories and Types of Dark Pattern Behavior

As mentioned previously, the guidelines list 15 types of dark patterns arranged into six broader categories. These categories are as follows:

- **Overloading.** The social media platform overwhelms users with large quantities of requests, information, options or possibilities to prompt them to share more data. The EDPB notes three types of dark patterns within this category: Continuous Prompting, Privacy Maze and Too Many Options.
- **Skipping.** The interface or user experience is designed in a way such that users forget or fail to consider some of the data protection aspects of their usage. Two types of dark patterns fall within this category: Deceptive Snugness and Look Over There.
- **Stirring.** Features that alter the choice users would otherwise make by appealing to their emotions or using visual nudges. Two types fall within this category: Emotional Steering and Hidden in Plain Sight.
- **Hindering.** Users are obstructed or blocked when they attempt to become informed about or manage their data or data settings by making the action hard or impossible to achieve. Three types fall within this category: Dead End, Longer Than Necessary and Misleading Information.
- **Fickle.** An interface design that is inconsistent and unclear, making it difficult for users to navigate the different data protection control tools available and understand the purpose of the data processing. Two types fall within this category: Lacking Hierarchy and Decontextualising.
- **Left in the Dark.** An interface designed in a way to hide information or tools devoted to data protection, or to otherwise leave users unsure of how their data is processed and what control they have over it regarding their rights. Three types fall within this category: Language Discontinuity, Conflicting Information and Ambiguous Wording or Information.

The following table (see page 4) sets out examples of dark pattern types from each of the six categories, along with a practical illustration of how the type may be encountered by a social media platform (SMP) user.

The guidelines have been published during a time of increased regulatory focus on deceptive design tactics used by consumer-facing platforms and websites. In October 2021, for example, the Australian Competition and Consumer Commission released an Interim Report focusing on the pre-installation of settings on mobile devices, with a specific focus placed on the dark patterns that nudge users into taking actions that may not be in their best interests. The FTC also has hosted a recent workshop on dark patterns seen in online marketplaces, noting that these patterns are beginning to emerge as a theme in consumer protection cases.

Key Takeaways

While the guidelines will be of particular use for providers of social media platforms, they also will be useful, practical guidance to all businesses that operate consumer-facing online businesses. In the guidelines, the EDPB draws particular attention to the GDPR's overarching principles of fairness and transparency that state personal data must not be processed in a way that is detrimental or unexpected to the data subject. Organizations must therefore ensure their websites and platforms provide comprehensive and easily accessible information about

personal data processing and data subject rights. While it may be tempting, for commercial reasons, to nudge customers to consent to more extensive processing, this may expose organizations to regulatory sanctions and financial penalties.

Dark Pattern Type	Category	Illustration
Privacy Maze. When users wish to obtain certain information, use a specific control or exercise a data subject right, they are forced to navigate through many webpages in order to obtain the relevant information or control, and there is no comprehensive and exhaustive overview available. Users are likely to give up trying or miss the relevant information or control.	Overloading	A user is able to make changes to a number of data processing settings on the SMP website, such as the extent to which data is shared with third parties. These settings are not, however, grouped in the same section of the website and the user must click through various tabs of their "Account" menu.
Deceptive Snugness. The most data-invasive features and options are enabled by default. Individuals are therefore "nudged" to keep a pre-selected option, and are unlikely to change this setting even if offered the possibility.	Skipping	When a user signs up for a new account on a SMP, the option "*share my posts with everyone*" is selected by default. The user must actively select an alternative option in order to share content with a smaller audience.
Emotional Steering. Using phrasing or visuals in a way that confers the information to users in either a highly positive outlook that makes users feel good or safe, or in a highly negative one that makes users feel scared or guilty. Influencing the emotional state of users in such a way is likely to lead them to take action that works against their data protection interests.	Stirring	A user of a SMP decides to delete their account. When navigating through the account deletion menu, various prompts attempt to discourage the user from their decision, such as: "*are you sure you want to give up all your connections?*" or "*it won't be the same without you*!"
Misleading Information. A discrepancy between information and actions available to users nudges them to do something they did not intend to. The difference between what users expect and what they actually get is likely to discourage them from going further.	Hindering	A user of a SMP on a desktop browser is invited to download the platform's mobile application. When they click the link, however, they are invited to enter a mobile phone number so they can be provided with a link to the application via text message.
Lacking Hierarchy. Information related to data protection lacks hierarchy; information may appear several times and be presented in several ways. Users are likely to be confused by this presentation and may be left unable to fully understand how their data is processed and how to exercise control.	Fickle	A SMP's privacy policy is 70 pages long and has no table of contents page or linked index.
Language Discontinuity. Information related to data protection is not provided in the official language(s) of the country where users live, whereas the service is. Users may, therefore, be unable to read the information and are likely to not be aware of how data is processed.	Left in the Dark	A Spanish-speaking user is able to freely access all the features of a SMP in Spanish. When searching for information about data protection, however, they discover that it is available only in English.

Return to Table of Contents

FDA Issues Proposed Guidance to the Health Care Sector on Medical Device Cybersecurity

The Food and Drug Administration (FDA) has released draft guidance on a modernized framework for cybersecurity applicable to medical device manufacturers and other health care sector stakeholders.

The FDA's guidance, titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," was released on April 8, 2022, in order to provide a concept of a modernized cybersecurity framework in response to increases in digital attacks targeting medical devices.[3] The guidance would replace a previous framework established by the FDA in 2018, and is open for public comment until July 7, 2022.

In the guidance, the FDA sets forth general security principles for medical devices and promotes the use of Secure Product Development Frameworks (SPDFs) to mitigate the frequency and severity of cybersecurity incidents that threaten patient care. Although the guidance is most directly applicable to medical device manufacturers (particularly those who file premarket submissions with the FDA), the principles and cybersecurity implications are useful for other key stakeholders. Health care facilities, providers and patients who use or work with medical devices also should consider the cybersecurity risks created or exacerbated by the interaction between medical devices and the medical or technology network in which the medical devices operate.

Background: Elevated Cybersecurity Risk in the Health Care Sector

The FDA highlighted several recent incidents that illustrate the need for a modernized approach to protecting medical devices, including the 2017 WannaCry ransomware attack that affected hospital systems and medical devices worldwide. In one example from this attack, the U.K.'s National Health Service reportedly experienced adverse effects on approximately 70,000 devices, resulting in deteriorated patient care. Since 2019, the FDA identified significant vulnerabilities in various commonly used third-party medical device components, such as URGENT/11 and SweynTooth. In 2020, a German hospital experienced a ransomware attack that was severe enough to force patients to be diverted to another hospital to receive emergency care.

The Details of the Guidance

Scope of Applicability

The guidance is applicable to (1) any medical devices containing software, firmware or other programmable logic and (2) software as a medical device (SaMD), and in each case, is applicable regardless of whether the medical device is network-enabled or not. Manufacturers of medical devices that require premarket submissions to the FDA will have to comply with the guidance (once finalized) in order to pass review. However, the guidance is written to apply more broadly to all devices within the scope of the Federal Food, Drug & Cosmetic Act. As such, manufacturers of medical devices for which a premarket submission is not required also should seek to implement the FDA's recommendations to mitigate risks of future incidents.

Four Core Principles for Medical Device Cybersecurity

The guidance describes four key principles of cybersecurity for medical devices:

- **Quality System Regulations (QSRs).** Device manufacturers must evaluate and comply with the QSRs set by the FDA that are applicable to the manufacturer's medical devices during the premarket or postmarket stage, or both (including software validation and risk analysis, particularly for network-enabled devices).
- **Designing for Security.** The adequacy of a medical device's security should be measured based on its ability to provide and implement the following security objectives throughout the system's architecture: authenticity and integrity; authorization; availability; confidentiality; and secure and timely updatability and "patchability."
- **Transparency.** Medical device users must receive sufficient information about medical devices to (a) securely integrate the medical device into the relevant use environment and network, and (b) maintain cybersecurity over the device's full life cycle. Examples of relevant information include undisclosed cybersecurity vulnerabilities or risks, configuration and update protocols, and risk exposure from communication interfaces or third-party software.
- **Submission Documentation.** Device cybersecurity design and documentation (as submitted to the FDA or maintained for users) must scale with the cybersecurity risk for that device and its intended and actual use environments. The documentation also must address how the risk varies when the device is used as a stand-alone instrument compared to when the device is used as a component of a network, system or protocol.

[3] See "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions." The guidance is intended to replace the prior framework set forth by the FDA in 2018, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

Secure Product Development Frameworks

The FDA recommends that that medical device manufacturers implement SPDFs to bring their cybersecurity approach into alignment with the four key principles described above. A proper SPDF is a set of processes designed to reduce the frequency and severity of product vulnerabilities and failure modes throughout a product's full life cycle, including development, release, support and decommission. A medical device developed through SPDF processes should have flexibility to address future changes to the cybersecurity risk landscape, including new intrinsic risks (*e.g.*, addition of connectivity-based features after marketing and distribution of the device) and extrinsic risks (*e.g.*, newly discovered exploitations or vulnerabilities in the device's use environment). The guidance includes detailed explanations of how a medical device manufacturer's SPDFs can complement and comply with QSR considerations, and also can inform the development of adequate user documentation and FDA submission materials.

Key Takeaways

Medical device manufacturers should review the cybersecurity principles set forth in the guidance (including as modified after the public comment period ends) and the FDA's recommendations to modernize the approach to cybersecurity risk mitigation throughout the life cycle of medical devices. Other key health care sector stakeholders also should strive to understand the guidance to better assess risk levels in their current medical device environment and appropriately vet devices in the future.

Return to Table of Contents

Colorado Attorney General Solicits Public Comments on Colorado Privacy Act Rulemaking

The Colorado attorney general is requesting public comments in connection with the Colorado Privacy Act (CPA), the state's comprehensive privacy law, prior to the beginning of the formal rulemaking process to occur during fall 2022.

Last year, on July 7, 2021, Colorado Gov. Jared Polis signed the CPA into effect, making Colorado the third state (after California and Virginia) to adopt a comprehensive privacy law.[4] The state's attorney general is responsible for the implementation and enforcement of the CPA and, accordingly, current Colorado Attorney General Phil Weiser is charged with the adoption of new rules to effect the CPA by July 1, 2023, including the technical specifications for one or more universal opt-out mechanisms. Although the formal rulemaking process is set to begin during fall 2022, Mr. Weiser announced on April 12, 2022, that his office is soliciting informal comments from the public to facilitate a productive and effective formal rulemaking process.[5]

In connection with the solicitation of informal comments, Mr. Weiser released the "Pre-Rulemaking Considerations for the Colorado Privacy Act" (the PRCs).[6] The PRCs provide guidance on key principles for the CPA rulemaking and specific, targeted questions that Mr. Weiser is seeking public input on.

Principles for CPA Rulemaking

The attorney general's office provided five key principles for CPA rulemaking to best implement in the CPA as enacted. Recommendations and concerns raised by informal comments will be reviewed in light of how each addresses or advances the key principles. The key principles are: (1) promote consumer rights; (2) clarify ambiguities; (3) facilitate efficient and expeditious compliance; (4) harmonize the CPA with other Colorado, state and federal laws; and (5) allow for innovation.

Key Issues for CPA Rulemaking

The PRCs lay out eight issues which the attorney general views as particularly crucial to the implementation of the CPA. Although Mr. Weiser invites input on any topic deemed relevant to the CPA, these are the issues viewed as most significant and thus most likely to result in specific rules and regulations.

- **Universal Opt-Out.** The CPA provides for so-called "universal opt-out mechanisms," which are technical measures by which consumers may exercise statutory rights to prevent the sale of their personal data or the processing of their personal data for targeted advertising. The CPA requires the Colorado attorney general to adopt rules containing technical specifications for at least one opt-out mechanism that data controllers (as defined in the CPA) can follow to comply with the law.
- **Consent.** The CPA requires consumer consent to the processing of personal data in certain circumstances, and includes high-level standards for what consent requires (a "clear, affirmative act"), while also identifying categories of conduct that cannot constitute consent (*e.g.*, acceptance of general terms). However, the attorney general intends to provide clarity around the policies and procedures a data

[4] The substantive aspects of the CPA, including comparisons with the California and Virginia privacy laws, were covered in our June 2021 *Privacy & Cybersecurity Update* article titled "*Colorado Expected to Become Third State to Adopt Comprehensive Privacy Law*."

[5] Informal comments to the Colorado attorney general regarding the CPA rulemaking can be submitted by clicking this link.

[6] The PRCs can be accessed here.

processer can adopt to demonstrate that they have obtained consent, as well as how special circumstances should be addressed (*i.e.*, consent by minors, compliance with another jurisdiction's consent requirements or changes in data policies).

- **Dark Patterns.** Dark patterns involve user interfaces that are designed to induce or manipulate a consumer to take a particular course of action. The CPA prohibits the use of dark patterns to obtain consent, and the rulemaking will provide further detail on what qualifies as a dark pattern in this context.
- **Data Protection Assessments.** Certain data processing activities pose a "heightened risk of harm to a consumer" under the CPA, including processing for the purpose of targeted advertising, selling personal data, processing sensitive data and processing for the purpose of profiling. Data controllers are required to conduct data protection assessments for any data processing posing a heightened risk of harm, and must provide those assessments to the attorney general upon request. The CPA rulemaking will address the requirements for adequate data protection assessments and the circumstances under which the attorney general can require a data controller to provide such assessments.
- **Profiling.** The CPA permits consumers to opt out of data profiling by which a data controller performs predictive analysis of the consumer that results in "legal or similarly significant effects," such as determinations related to financial or lending services, housing, insurance, employment or health care. The attorney general is seeking feedback on what type of transparency would enable consumers to understand this profiling and make informed opt-out decisions, as well as specific types of profiling that may require special rules.
- **Opinion Letters and Interpretive Guidance.** The CPA authorizes the attorney general to design a process by which it can issue opinion letters and interpretive guidance regarding compliance with the CPA and the rules promulgated by the attorney general. The attorney general is seeking guidance on the elements of this process.
- **Offline and Off-Web Collection of Data.** The CPA covers data regardless of the collection mechanism, whether collected online or offline (digitally or physically). The attorney general is seeking input on how the CPA's requirements might apply to the offline collection of data.
- **Protecting Coloradans Nationally and Globally.** The CPA rulemaking may address how the law interacts with, differs from or conflicts with the laws of other states, federal law and laws of foreign nations.

Key Takeaways

Relevant stakeholders whose interests are implicated by the CPA and the rules to be promulgated by the attorney general should monitor the current informal pre-rulemaking comment period and the formal notice-and-comment period during fall 2022. The rules developed by the attorney general will directly affect individual data privacy rights and the regulatory regime that data controllers must comply with.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000