Skadden

Privacy & Cybersecurity Update

FTC to Focus on Protection of Consumers' Location, Health and Other Sensitive Data

A Federal Trade Commission (FTC) official published a post on the FTC's Business Blog suggesting that the commission will focus on enforcing laws that protect consumers' location, health and other sensitive data.

On July 11, 2022, Acting Associate Director of the FTC Division of Privacy & Identity Protection Kristin Cohen posted an article to the FTC's Business Blog highlighting the dangers posed by the increasing amount of consumer health and location data being collected.[1] The post suggested that the FTC will focus on protecting this data in future enforcement actions, with Ms. Cohen concluding the post by giving advice to companies to avoid running afoul of the commission.

Background

The post first enumerated the numerous connected devices that track people's precise location and health information, and noted that the privacy risk is exacerbated by the aggregation of data from different sources, the data's increasing granularity and scale driven by adtech and data brokers, and the prospect of increasing generation and collection of user-generated health data. Taken together, Ms. Cohen stated that this "potent combination of location data and user-generated health data creates a new frontier of potential harms to consumers."

Ms. Cohen also warned that the marketplace for this data is "opaque." According to the post, once the data is collected using mobile operating systems and embedded tools in mobile apps, it goes to a sales floor where it is bought and sold by multiple parties. The data then reaches data aggregators and brokers who combine data from different sources and sell it to marketers, researchers and, sometimes, government agencies. The post emphasized the unprecedented scale of the data and increasingly sophisticated inferences that can be made from it, once combined.

[1] The blog post is available here.

Past Enforcement

Ms. Cohen cited two examples of "misuse" of health data. In 2017, the Massachusetts attorney general settled with a marketing company, Copley Advertising, LLC, that used location technology to send advertisements about alternative options to people who crossed a "secret digital 'fence'" when visiting an reproductive health clinic. In the case, the attorney general claimed that Copley Advertising had violated state laws related to consumer protection. Additionally, the post discussed the FTC's settlement with Flo Health, which allegedly shared information from its app about women's periods and fertility tracking, in spite of promises to keep the information private. The post came days after an executive order from President Joe Biden that directed the FTC to "protect consumers' privacy when seeking information about and provision of reproductive healthcare services."

The post stated that the misuse of location and health data exposes consumers to "significant harm" and that the FTC will "us[e] the full scope of its legal authorities to protect consumers' privacy." According to the post, the FTC also "will vigorously enforce the law if [it] uncover[s] illegal conduct that exploits Americans' location, health, or other sensitive data," while also pointing to the FTC's past enforcement actions as a road map for companies.

Advice for Companies

After discussing concerns about location and health data, the post advised companies who collect confidential consumer data on how to comply with the law. These strategies are outlined below.

- **Several federal and state laws protect sensitive data.** The post underscored the several state and federal laws that control the "collection, use and sharing of sensitive consumer data." Specifically, Ms. Cohen mentioned (1) the FTC's ability to enforce Section 5 of the FTC Act that "broadly prohibits unfair and deceptive trade practices"; (2) the Safeguards Rule, which regulates measures to keep consumer data secure by financial institutions under FTC jurisdiction; (3) the Health Breach Notification Rule, which mandates certain customer notification following a data breach of personal health records; and (4) the Children's Online Privacy Protection Rule, which regulates websites that are directed to children under 13 years old. The post noted that some FTC cases have involved large civil penalties.
- **Claims involving data anonymization may often be deceptive.** The post made clear that false claims about anonymizing user data will be treated as a "deceptive trade practice" and will violate the FTC Act. Moreover, Ms. Cohen wrote that research has demonstrated that "anonymized" data can often be reidentified, particularly regarding location data. She also noted that false claims about anonymization will be pursued by the FTC.
- **The FTC takes "misuse" of consumer data seriously.** Ms. Cohen warned that the FTC will not allow companies to "over-collect, indefinitely retain, or misuse consumer data." The post cited recent examples to bolster this point, including the collection of location data from children without parental consent; a company's indefinite retention of "sensitive consumer data," among other violations; and the improper collection and retention of consumer data, in spite of consumer requests for deletion.

Throughout the post, Ms. Cohen outlined remedies involving millions of dollars in fines, the deletion of offending data and, in one case, the deletion of work product algorithms made using the offending data.

Key Takeaways

Ms. Cohen's blog post — though not an official statement by the FTC — suggests that the commission is looking to focus on these issues in the near future through enforcement or other measures. Companies that collect and utilize location and health-related data should ensure that they comply with existing federal and state laws and that they accurately communicate the ways in which they use this data.

Return to Table of Contents

Plaid to Pay $58 Million to Settle Data Claims

The maker of the financial services application Plaid, which is used by many popular financial technology applications, has agreed to pay $58 million to settle a class action claim arising from its data collection and use practices.

On July 20, 2022, a federal judge approved a $58 million settlement of certain data collection and use claims against Plaid, Inc., which provides login services for banking applications, and linking and verification services for various financial technology applications.[2] The plaintiffs had claimed that Plaid harvested and sold their financial information without their knowledge or consent, while the company has asserted that it had already discontinued the practices that gave rise to the complaint.

Background

Plaid provides a service that connects bank accounts to other financial technology services, and is used by a wide array of popu-

[2] The settlement agreement is available here.

lar investment and money transferring applications. Plaid's service enables people to link their bank accounts to these other services so that users can add funds to their various accounts on such service providers, as well as withdraw funds from these services into their bank accounts.

According to the plaintiffs, Plaid did not adequately notify them that they were providing their banking credentials to the company rather than to their banks. They also claimed that Plaid designed login screens to resemble those of the banks, thus further obscuring its involvement. Finally, the plaintiffs alleged that Plaid used the accumulated bank login information in order to collect a significant amount of consumer banking data that it then routinely sold to third parties.

Settlement

The settlement agreement was preliminarily approved in November 2021 and finally approved in July 2022. Under the terms of the agreement, Plaid will pay $58 million into a fund to be paid out to members of the class, after deducting attorneys' fees and costs, taxes and certain administrative expenses.

In addition, Plaid agreed to certain changes to its data collection practices, including:

- **Data deletion.** Plaid must delete certain transaction-related data that it collected related to users that did not connect a bank account to an application that requested that data. The company also must delete data related to users that it can no longer authenticate with the financial institution (*e.g.*, if the password has changed or the account has been closed).
- **Plaid Portal.** Plaid has launched a product known as Plaid Portal that provides the same functionality as its original service (linking back accounts to financial applications), but is more clearly identifiable as being provided by Plaid, and includes more user control over certain privacy settings and the ability to delete certain data. Under the settlement, Plaid will prominently disclose that users can create Plaid Portal accounts and will periodically remind Plaid Portal account holders of the privacy tools available to them.
- **Disclosures in Service.** Plaid must make certain changes to its basic linking service to (1) provide clearer notice and consent to its privacy policy, referring expressly to Plaid's role in linking accounts, and (2) ensure that the background colors it uses on the page in which users enter their credentials does not match the color used by the corresponding financial institution.
- **Privacy Policy Changes.** Plaid must update its privacy policy to provide more detailed information about the data it collects, and how it uses and shares that data.
- **Data Minimization.** Plaid must minimize the data it stores from users' financial accounts by (1) only storing the data that the user's application specifically requests or that is necessary for Plaid to provide its service (unless the user has expressly consented to the retrieval of additional fields), and (2) continuing to inform the applications that use Plaid about functionality that terminates the customer's access to data and that will result in deletion of data unless it used by another customer.

Plaid denied the allegations of privacy violations and the settlement agreement does not include any admission of wrongdoing by the company. Additionally, in public statements surrounding the settlement, Plaid indicated that the claims in the suit were about its prior policies and practices, and that it is already doing many of the things required by the settlement.

Return to Table of Contents

UK Government Calls for Input on the Regulation of Data Infrastructure and Publishes Review of Existing Network Information System Regulations

The U.K. government has requested input on the nation's data storage and processing infrastructure, and published its second post-implementation review of the Network Information Systems (NIS) Regulations 2018.

On June 22, 2022, the U.K. government launched a consultation on the nation's data storage and processing infrastructure, including data center, cloud platform and managed service provider infrastructure.[3] Additionally, on July 27, 2022, the government released a report of its review of the NIS Regulations 2018. Together, these developments reflect the government's continued focus on establishing appropriate legal mechanisms for protecting and ensuring the stability of the country's data infrastructure.

Background

As addressed in previous *Privacy and Cybersecurity Updates,*[4] the government has already noted the critical importance of the U.K.'s data infrastructure in its National Data Strategy (published September 2020) and National Cyber Strategy (published December 2021), and affirmed its commitment to creating a stronger risk management framework. The enhanced protection afforded to the U.K.'s infrastructure, which is considered a "vital national asset," will, according to the consultation, help support

[3] The consultation is available here.

[4] See our January *2022 Privacy & Cybersecurity Update* article "UK Government Publishes National Cyber Strategy" and our June *2022 Privacy & Cybersecurity Update* article "UK Government Announces a Six-Point Digital Strategy."

a "pro-growth and innovation-friendly economy" that expands the use of data and technology without posing a threat to privacy and security. The press release launching the consultation stated that this expansion is well underway, noting that between 2013 and 2019 the number of businesses purchasing cloud services doubled and 53% of businesses now rely on cloud platforms.

The Consultation

The government's stated priorities in running the consultation are two-fold. Firstly, the government recognizes the strategic importance that data has in the U.K. economy. The nation's data infrastructure, which plays host to large volumes of valuable and sensitive data, may therefore be an attractive target to individuals and organizations seeking to attack the U.K.'s economy or national security. Secondly, the government notes the increasing reliance of the U.K. upon data storage and processing services for its essential services and the functioning of the wider economy.

The government's view is that despite the essential nature and recent growth of the nation's data infrastructure, its security and resilience is still relatively unregulated. Data centers may be subject to the NIS Regulations (*e.g.*, if they are cloud platform providers), the U.K. GDPR or under other regulation(s) indirectly, including because they process data belonging to customers in more heavily regulated sectors (*e.g.*, health care or finance).

The consultation reiterates the government's commitment to the development of a stronger risk management framework, focusing on the risks associated with data storage and processing infrastructure. These risks, if left unchecked, may lead to: (1) unwanted access by bad actors to large volumes of data stored in the U.K.'s data infrastructure and (2) market disruption due to data infrastructure acting as a "single point of failure" for essential services and the broader economy. The latter case was illustrated recently in July 2022, when the U.K. experienced some of the hottest temperature days on record and heat-triggered outages were experienced by a number of data centers, including those serving hospitals and other essential services.

The consultation seeks views on various questions and proposals aimed at improving defense, resilience and recovery factors, and asks respondents to assess the sector's risk management measures. It also identifies a number of proposals that may be introduced under future regulations or legislation, including legal requirements regarding:

- defined and tested service continuity assurances and incident management plans, to be engaged in the result of system failures;
- appropriate and proportionate measures to identify and manage security and resilience risks;
- notification of a regulator in the event of a material outage or incident, or during the course of an investigation;
- accountability and governance, including a requirement to appoint a suitable individual at the board-level to oversee security and resilience; and
- penetration testing, including proposals that attempted breaches be carried out by government authorities or competent third parties.

Originally scheduled to close on July 24, 2022, the deadline to submit views has been extended and the consultation will now close on August 8, 2022.

Review of NIS Regulations

The consultation represents an important step in the government's push towards stricter regulation of data storage and processing infrastructure, with the results likely to underpin more significant government oversight of the sector in the future. It is not the only step, however; in July 2022, the government published its second post-implementation review of the NIS 2018 Regulations, which were designed to protect digital and essential services from cyberattack.[5] The review notes that there is "room for improvement" in the NIS Regulations, and proposes a number of amendments to the regulatory regime, including providing for greater flexibility in the scope of organizations under its purview, increased management of supply chain risk and greater resource allocation for enforcement.

Key Takeaways

The consultation and review of the NIS Regulations show a general trend towards heightened regulation of data infrastructure and also may serve as a reminder of the critical role that the government plays in the majority of businesses, regardless of size. Organizations should ensure that operational and legal diligence processes are in place to evaluate data storage and processing providers, and that business units undertake regular reviews of relevant suppliers.

Return to Table of Contents

[5] The report is available here.

UK Data Protection Regulator Announces Plan to Reduce Business Compliance Costs

The U.K. Information Commissioner's Office (ICO) has announced a wide-ranging three-year plan for data protection, which includes measures designed to save businesses more than £100 million in privacy compliance costs.

On July 14, 2022, the ICO unveiled its high-level strategic objectives for the next three years, including a detailed action plan for October 2022 to October 2023.[6] In keeping with the various sectors and stakeholders that the ICO governs, the plan — dubbed "ICO25" — addresses a wide array of topics, ranging from safeguarding children's rights to addressing cost-of-living concerns. For U.K. businesses and businesses that serve U.K.-based customers, key elements of ICO25 are the practical action items designed to save businesses over £100 million before 2025, including publication of templates and guidance designed to reduce the cost of compliance. ICO25 is open to public consultation until September 22, 2022.

Background

Information Commissioner John Edwards launched ICO25 in a speech that highlighted both the (1) opportunities to private sector businesses in "empowering organisations to use information responsibly and confidently to invest and innovate" and "empowering people to confidently share their information to use the products and services that drive our economy and society," by creating more clarity and certainty with respect to compliance and enforcement, and (2) risks to noncompliant private sector businesses of being "on the receiving end of [the ICO's] most punitive tools," which aligns with the U.K. government's intention to raise the maximum level of Privacy and Electronic Communications Regulations (PECR) fines to those outlined under the U.K. GDPR.

Key ICO25 Initiatives for the Private Sector

ICO25 covers a broad range of initiatives, including the following from a private sector business perspective:

Affordable and User-Friendly Compliance Tools

The ICO proposes to reduce business data protection compliance costs by providing the following:

- **Training Materials.** On its website, the ICO will publish its existing internal data protection and freedom of information training materials, along with a newly developed range of "data essentials" training materials aimed at small- and medium-sized businesses for which data processing does not form a part of their core activities.
- **Advice Database.** The ICO will create a number of databases of the advice provided to businesses, including the "one-off" advice provided to anonymous organizations and members of the public (*e.g.*, through the ICO's free telephone service), and the recommendations made to organizations following complaints, investigations and audits.
- **Compliance Templates.** In addition to those templates already made available on their website (*e.g.*, the data protection impact assessment template), the ICO will produce a range of off-the-shelf products and templates to help organizations develop their own compliance programs.
- **Sector-Specific Advice.** The ICO will work with sector-specific ombudsman and representative groups to co-design tailored and targeted compliance advice for various sectors.
- **Support for Innovation.** The ICO will provide bespoke support and regulatory clarity to innovative businesses working with personal data, with the introduction of a new service called "iAdvice." ICO25 also notes the ICO's intention to develop a data subject access request (DSAR) tool to enable individuals to generate an instant DSAR. According to the ICO, this would make the process of requesting access to data simpler and clearer for both the data subject and the organization receiving the request.

Enforcement

Enforcement is an important ICO mechanism that aims to encourage data protection compliance and protect the most vulnerable data subjects. ICO25 explains that the ICO will prioritize the following enforcement-related issues over the next year:

- **Response and Resolution Times.** ICO25 includes a number of key performance indicators centered around response and resolution times for claims and investigations, including a commitment to conclude 95% of all formal investigations within 12 months, ensure 90% of audit recommendations are accepted in full or in part, to assess and respond to 80% of complaints from data subjects within 90 days, refer or close 80% of personal data breach reports within 30 days, and resolve 80% of written enquiries within seven days. To meet these key performance indicators, the ICO may utilize its enforcement power to require businesses to be more responsive.
- **Approach to Enforcement.** ICO25 notes that the agency will consider the potential risk posed or actual harm caused when selecting an enforcement action. While still unclear, this may mean that administrative fines will be reserved for

[6] ICO25 is available here.

more serious violations instead of remedial actions, audits or monitoring. Unlike the decision to relax public authority enforcement for two years, the ICO has not communicated the same with respect to private sector businesses. This may signal the start of a sector-specific approach to enforcement by the ICO, especially given the information commissioner's comments on topic.

AI-Driven Discrimination

The ICO will further examine how to combat AI-driven discrimination by sharing updated guidance with AI developers to ensure their software algorithms treat people and their information fairly, while also seeking to actively investigate circumstances where AI is having a discriminatory effect (*e.g.*, AI tools used for recruitment or eligibility for financial support). Given the increased use of AI in automated business processes, companies may increasingly want a commitment from their suppliers that they have taken steps to ensure their AI is nondiscriminatory.

Children

In line with U.K. government initiatives (*e.g.*, the Online Safety Bill), the ICO has continued to focus on children's privacy rights, in particular in relation to internet-based interactions. While there will be a heavier focus on social media platforms, video and music streaming sites and gaming platforms, any business with an online presence will have an obligation to ensure that children have an age-appropriate online experience.

Key Takeaways

Determining whether — and to what extent — the plans described in ICO25 will have a positive effect on business will be determined by how the ICO roll out their strategies. From the plans the ICO has shared to date, we can note:

- Whilst the ICO's plans include a commitment to implement a package of actions that are intended to reduce the cost and complexity of data protection compliance for businesses, the ICO25 announcement was accompanied by a clear warning to those that misuse personal data.
- The information commissioner also noted that upcoming legal reforms[7] to the U.K.'s data protection regime will allow the ICO to devote more of its resources towards discretionary matters and internally generated investigations (*e.g.*, into predatory marketing), whereas a significant proportion of its current workload is dedicated to responding to complaints. In the July 2022 Data Protection Practitioner's Conference, the information commissioner flagged his interest in broadening its scope to determine data subjects' compensation claims (which are currently resolved via litigation). Given that a number of ICO25 key performance indicators focus on response and resolution timings, it will be interesting to see how the ICO intends to manage these potential increases to its caseload volume.

[7] See our May 2022 *Privacy & Cybersecurity Update* article "Queen's Speech Confirms Planned Overhaul of UK Data Protection Regime."

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

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@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

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