2023 YEAR IN REVIEW

The Year That Was: Key Cybersecurity and Privacy Developments in 2023 and Issues for 2024

Paul, Weiss, Rifkind, Wharton & Garrison LLP

Paul | Weiss

December 28, 2023

The Year That Was: Key Cybersecurity and Privacy Developments in 2023 and Issues for 2024

At the beginning of the year, we predicted that the use of personal information and the protection of data in an evolving threat environment would be the focus of increased legislation, regulation, and regulatory enforcement. And 2023 delivered, with both threat actors and regulators presenting new challenges for technology and legal teams. At the same time, these teams are navigating how to harness the burgeoning potential of rapidly evolving artificial intelligence applications while mitigating associated security, legal, and related risks. Amidst all of the noise, the Paul, Weiss Cyber & Data Protection team breaks down below ten key developments of 2023 that contributed to an increasingly complex legal and data security landscape and prompted business leaders to increase resources and attention to bolster their defenses and ensure compliance with their growing list of legal obligations. We predict a continued flurry of activity in 2024.

1. California and Its Privacy Protection Agency Move Forward with New Laws and Regulations Limiting the Collection and Use of Personal Information, with More Enforcement and Regulations to Come

California continues to push forward with data privacy legislation and regulation, with the California Privacy Protection Agency ("CPPA") adopting its first rulemaking package under the California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA"). The new rules regulate and limit the collection of personal information by entities covered by those laws, and require that regulated entities follow principles of data minimization.[1] The CPPA expects to begin enforcement actions under the new regulations as soon as March 2024.[2]

In addition, on October 10, 2023, Governor Newsom signed the Delete Act, which will provide residents of California with access to a "one-stop-shop" mechanism to request the deletion of their data by data brokers operating in the state. The mechanism must be developed by the CPPA by January 1, 2026.[3]

On November 27, 2023, the CPPA proposed broad-reaching regulations restricting certain applications of artificial intelligence, or "automated decision-making technology" ("ADMT"), which is defined as "any system, software, or process — including one derived from machine-learning, statistics, or other data-processing or artificial intelligence — that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decision

1 *See* California Privacy Protection Agency, *California's Office of Administrative Law Approves CCPA Regulations* (Mar. 30, 2023), https://cppa.ca.gov/announcements/2023/20230330.html.

2 *See Cal. Chamber of Commerce* v. *Cal. Priv. Prot. Agency*, No. 34-2023-80004106, at 5 (Cal. Super. Ct. June 30, 2023) (staying enforcement of regulations until 12 months from the date that the regulations become final).

3 2023 Cal. Legis. Serv. ch. 709 (West).

making."[4] The proposal would require notice before the use of consumer data for automation, mandate disclosures about the technology's purpose, and provide opt-out rights. The CPPA is also considering risk assessment requirements that would "work in tandem" with the ADMT regulations. Both sets of regulations were discussed at a December 8, 2023 CPPA Board meeting.[5]

2. Beyond California: Other State Data Privacy Laws

Comprehensive data privacy legislation: Following the path first blazed by California, seven states enacted comprehensive data privacy laws in 2023. Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, and Texas joined Colorado, Connecticut, Virginia and Iowa, which already had laws on the books. The proliferation of laws in these various states have created a complex patchwork of protections, definitions, and carveouts for businesses to decipher and navigate. For example, the Colorado Privacy Act, which came into effect on July 1, 2023, includes nonprofit organizations—a category not covered under many other state laws—and defines religious beliefs, information relating to sex life or sexual orientation, and citizenship status as "sensitive" data that must be collected in adherence with strict consent rules.[6] Oregon's Consumer Privacy Act, which comes into effect on July 1, 2024, also includes status as transgender or nonbinary, and status as a crime victim, as "sensitive" data.[7] The Tennessee Information Protection Act, which comes into effect on July 1, 2025, is innovative in its reference to the NIST Privacy Framework as a possible safe harbor for businesses.[8] Businesses that collect data from residents of these states need to take steps to ensure that they understand and comply with these laws, including putting in place appropriate privacy and data security policies.

Health data protection: Washington state enacted the My Health My Data Act to provide consumers with broad protections of their health data — including both location data related to health care and, arguably, information about food and hygiene product choices. The Washington law creates a private right of action for consumers and patients, and will apply to entities not covered by the federal Health Insurance Portability & Accountability Act ("HIPAA"), including online health apps.[9] In the wake of the U.S. Supreme Court decision in *Dobbs*, we expect other states may follow Washington's lead in providing additional protections for certain categories of health data.

Social media regulation: Florida enacted a "Digital Bill of Rights" that in some ways is similar to the comprehensive data privacy bills passed recently in other states. For example, the law provides consumers with the right to opt out of the sharing of their data, to be notified of data collection, and to consent to the sale of their data to brokers. But the Florida law applies only to large technology companies with over $1 billion annual revenue. Further, in addition to providing data subjects with certain data privacy rights, the law requires companies that operate search engines to disclose how their content moderation "prioritize[es] or deprioritize[es] political partisanship or political ideology in search results."[10]

Limiting access by children: Finally, several states passed legislation purporting to protect children by limiting minors' access to social media. But the fate of these laws is uncertain in the wake of several federal lawsuits that raise First Amendment concerns that requiring websites to collect age verification from adult users constitutes an unconstitutional prior restraint of legal speech.

---

4 California Privacy Protection Agency, *A New Landmark for Consumer Control Over Their Personal Information: CPPA Proposes Regulatory Framework for Automated Decisionmaking Technology* (Nov. 27, 2023), https://cppa.ca.gov/announcements/2023/20231127.html; California Privacy Protection Agency, *Draft Automated Decisionmaking Technology Regulations* (Dec. 2023), https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf.

5 California Privacy Protection Agency Board, *Meeting Notice & Agenda*, https://cppa.ca.gov/meetings/agendas/20231208_agenda.pdf.

6 Colo. Rev. Stat. § 6-1-1303(24) (2021). *See generally* 2021 Colo. Legis. Serv. ch. 483 (West).

7 2023 Or. Legis. Serv. ch. 369 § 1(18)(a) (West).

8 Tenn. Code Ann. § 47-18-3213 (2023). *See generally* 2023 Tenn. Legis. Serv. ch. 408 (West).

9 Wash. Rev. Code §§ 19.373.010(8)(a), 19.373.900 (2023). *See generally* 2023 Wash. Legis. Serv. ch. 191 (West).

10 Fla. Stat. §§ 501.702(9), 501.71(4). *See generally* 2023 Fla. Sess. Law Serv. ch. 2023-201.

State legislation targeting access to pornography has been blocked on similar grounds, but other state laws that provide a private right of action against adult websites without compliant age verification have been upheld.

- **California**: U.S. District Judge Beth Labson Freeman granted a preliminary injunction to block enforcement of the Age-Appropriate Design Code Act ("AADC"). She concluded that age-gated restrictions to online information have a chilling effect, and they likely fail the First Amendment's strict scrutiny standard.[11]

- **Texas**: U.S. District Judge David Alan Ezra granted a preliminary injunction against the state of Texas enjoining it from enforcing its age verification law targeting pornography websites, known as HB 1181. He found that the statute did not stand up to the First Amendment's strict scrutiny standard, in part due to the chilling effect created by the risk of data breaches exposing website visitors' identities.[12]

- **Arkansas**: U.S. District Judge Timothy L. Brooks granted a preliminary injunction in favor of tech advocacy group NetChoice enjoining the enforcement of the state's Social Media Safety Act. He held that the law, which requires some online social media platforms to verify the ages of all new users and obtain parental consent for children creating accounts, was not narrowly tailored to its goals.[13]

- **Utah**: U.S. District Judge Ted Stewart dismissed a lawsuit against the Utah State Attorney General and the Commissioner of the Utah Department of Safety seeking to enjoin them from enforcing of Utah's Social Media Regulation Act, which requires age verification for adult websites. He held that the state officials could not be sued because the law's enforcement mechanism is a private right of action by residents.[14]

- **Louisiana**: U.S. District Judge Susie Morgan dismissed a pre-enforcement challenge to Act 440, an age-verification law for adult websites. She concluded that the challenge was barred by sovereign immunity due to the law's private right of action, and that the plaintiffs lacked standing to bring the challenge.[15]

3. National Cybersecurity Strategy

On March 2, 2023, the Biden Administration announced its updated National Cybersecurity Strategy (the "Strategy") "to secure the full benefits of a safe and secure digital ecosystem for all Americans." The Strategy calls for stronger regulation of cybersecurity, more counter-hacking activity by law enforcement, and greater accountability for software manufacturers, in order to "realign incentives" to protect national security, public safety, and economic prosperity.[16] Improved private-public collaboration is at the core of the Administration's vision for protecting critical infrastructure, although the Strategy aims to achieve that collaboration in part through increased regulation and new legislation allowing software providers to be held liable for releasing products that are not secure by design. In an era of congressional gridlock, the aspects of the Administration's strategy that can be implemented by executive action alone have drawn the greatest focus.

---

11 *NetChoice, LLC* v. *Bonta*, No. 22-cv-8861, 2023 WL 6135551 (N.D. Cal. Sept. 18, 2023).

12 *Free Speech Coal., Inc.* v. *Colmenero*, No. 1:23-cv-917, 2023 WL 5655712 (W.D. Tex. Aug. 31, 2023).

13 *NetChoice, LLC* v. *Griffin*, No. 5:23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023).

14 *Free Speech Coal., Inc.* v. *Anderson*, No. 2:23-cv-287, 2023 WL 4899509 (D. Utah Aug. 1, 2023).

15 *Free Speech Coal., Inc.* v. *LeBlanc*, No. 23-cv-2123, 2023 WL 6464768 (E.D. La. Oct. 4, 2023).

16 The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy* (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/; *see also* The White House, *National Cybersecurity Strategy* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

In July, the Biden Administration released its implementation plan for the Strategy, identifying 65 initiatives led by 18 different departments and agencies.[17] While there has been progress on some of the initiatives—for example, in September the FCC, released a notice of proposed rulemaking seeking comment on a proposed voluntary cybersecurity labeling program for Internet of Things (IoT) devices or products[18]—the time horizon for many initiatives is much longer. For example, CISA is not expected to issue final rules pursuant to the Cyber Incident Reporting for Critical Infrastructure Act until the end of FY2025. Although there is much work to do, the implementation plan's clear assignment of responsibility and expected completion dates for each initiative provides a preview of the cyber regulatory agenda for the next several years.

4. SEC, FTC, and State Regulators Implement New Cybersecurity and Incident Disclosure Rules

Federal and state regulators promulgated new rules requiring increased disclosure of cybersecurity incidents.

In July, the Securities and Exchange Commission adopted new disclosure requirements to enhance and standardize public company disclosures regarding cybersecurity risk management and incident reporting.[19] Among other requirements, companies will be required to disclose material cybersecurity incidents within four business days on Form 8-K, and to provide annual disclosure regarding their cybersecurity governance and risk management.[20]

Relatedly, on March 15, 2023, the SEC unanimously proposed amendments to enhance Regulation S-P's provisions requiring registered investment advisers ("RIAs") to protect customer (e.g., certain fund limited partners) information.[21] The proposal would amend Regulation S-P to require RIAs to adopt a written incident response program reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information, and would require customer information breach notifications.[22] Final action on the proposal is expected in April 2024.

The Federal Trade Commission also has imposed notification requirements for breaches by updating its Safeguards Rule to require notification "where unencrypted customer information involving 500 or more consumers is acquired without authorization." The revised rule covers non-banking financial institutions such as mortgage brokers and will come into effect on May 13, 2024.[23]

The New York State Department of Financial Services (NYDFS) also finalized updates to its cybersecurity regulations, known as Part 500.[24] The now-final regulations strengthen the obligations imposed on NYDFS-regulated financial entities to report

---

17 The White House, *National Cybersecurity Strategy Implementation Plan* (July 2023), .

18 Cybersecurity Labeling for Internet of Things, 88 Fed. Reg. 58211 (Aug. 25, 2023).

19 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023).

20 *See also* Paul, Weiss, *SEC Adopts New Cybersecurity Disclosure Requirements* (Aug. 2, 2023), https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/sec-adopts-new-cybersecurity-disclosure-requirements?id=47481.

21 Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 88 Fed. Reg. 20616 (Apr. 6, 2023).

22 Paul, Weiss, *SEC Proposes Enhancements to Regulation S-P: Potential Implications for Private Fund Advisers* (Mar. 20, 2023), https://www.paulweiss.com/practices/transactional/investment-management/publications/sec-proposes-enhancements-to-regulation-s-p-potential-implications-for-private-fund-advisers?id=46305.

23 *Standards for Safeguarding Customer Information*, 88 Fed. Reg. 77499 (Nov. 13, 2023).

24 45 N.Y. Reg. 23 (Nov. 1, 2023).

cybersecurity events and to protect consumer data, and will require such entities to make larger investments in cybersecurity infrastructure.[25]

And the New York State Department of Health proposed cybersecurity regulations for hospitals. The new rules would complement the protections of HIPAA for patient records by requiring hospitals to establish a cybersecurity program, and develop response plans for potential cybersecurity incidents.[26]

5. FTC and HHS Bring Federal Enforcement Actions

The FTC flexed its authority under Section 5 of the FTC Act to protect consumers in the digital privacy space. For example, the agency's ongoing enforcement action against data broker Kochava tests whether the agency can prove sufficient harm under Section 5 based on the company's sale of comprehensive data sets, including geolocation data, obtained from consumer mobile devices.[27]

In another example of the FTC regulating what it views as the improper sharing of consumer data, on May 17, 2023, Easy Healthcare Corporation, which operates the ovulation tracking app Premom, settled with the FTC for $200,000 for unlawfully sharing user data with third parties. The FTC also found that, by failing to notify users about the data disclosures, Premom violated the FTC's Health Breach Notification Rule, which applies to businesses not covered by HIPAA.[28]

The FTC is also investigating so-called "dark patterns" in digital user interfaces that it views as limiting consumers' ability to provide full and informed consent for data collection and subscription renewals. For example, the agency recently obtained approximately $100 million in refunds for Vonage customers who were improperly prevented from canceling their service subscriptions.[29] And on June 26, 2023, the agency settled, for $18.5 million, its claims against Publisher's Clearing House (PCH) alleging that customers were misled by PCH's manipulative phrasing and website design into purchasing products to improve their chances to win prizes.[30]

On June 5, 2023, the FTC settled with Microsoft for $20 million for alleged violations of the Children's Online Privacy Protection Act (COPPA). The FTC's complaint alleged that Microsoft collected personal data of children through Xbox Live without obtaining parental consent, retained this data for longer than necessary, and allowed children to upload photographs to their profiles.[31]

---

25 Paul, Weiss, *NYDFS Finalizes Updates to Part 500 Cybersecurity Regulation* (Nov. 8, 2023), https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/nydfs-finalizes-updates-to-part-500-cybersecurity-regulation?id=49006.

26 Governor Kathy Hochul, *Governor Hochul Announces Proposed Cybersecurity Regulations for Hospitals Throughout New York State* (Nov. 13, 2023), https://www.governor.ny.gov/news/governor-hochul-announces-proposed-cybersecurity-regulations-hospitals-throughout-new-york.

27 Am. Compl., *Federal Trade Commission* v. *Kochava Inc.*, No. 2:22-cv-00377 (D. Idaho June 5, 2023).

28 Federal Trade Commission, *Ovulation Tracking App Premom Will Be Barred from Sharing Health Data for Advertising Under Proposed FTC Order* (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

29 Federal Trade Commission, *FTC Sends Nearly $100 Million in Refunds to Vonage Consumers who Were Trapped in Subscriptions by Dark Patterns and Junk Fees* (Oct. 30, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-sends-nearly-100-million-refunds-vonage-consumers-who-were-trapped-subscriptions-dark-patterns.

30 Federal Trade Commission, *Publishers Clearing House Refunds* (Nov. 2023), https://www.ftc.gov/enforcement/refunds/publishers-clearing-house-refunds.

31 Federal Trade Commission, *FTC Will Require Microsoft to Pay $20 Million Over Charges It Illegally Collected Personal Information from Children Without Their Parents' Consent* (June 5, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information.

The Office for Civil Rights of the Department of Health and Human Services, which is charged with enforcing the HIPAA Privacy Rule, was also active in 2023. It settled many cases, including ones in which patients' personal health information was stolen in cyberattacks, accessed by unauthorized employees, or provided to a news outlet reporting on the Covid-19 pandemic.[32]

6. The EU-U.S. Data Privacy Framework Comes into Force

The finalization of the EU-U.S. Data Privacy Framework ("DPF") now provides companies with a mechanism to transfer data between the U.S. and the EU in compliance with the GDPR, pursuant to the European Commission's adequacy decision on July 10, 2023.[33] In July, the U.S. Department of Commerce launched a "one-stop-shop" website providing information about the DPF.[34]

We expect companies currently using standard contractual clauses and binding corporate rules to transfer EU personal data to the United States to migrate to the DPF, although some may await the resolution of challenges in EU courts that may address whether the DPF is sufficient to adequately protect EU data subjects data under the GDPR.

7. Executive Order on Artificial Intelligence

On October 30, 2023, the Biden Administration issued its "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" ("EO"), calling for safeguards for the privacy of Americans' data and for agencies to assess the risks posed by artificial intelligence to national security.[35] The order directs the federal government to "ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks" using available technical and policy tools.[36]

Among various cybersecurity efforts included in the EO, the Secretary of Commerce is directed to propose regulations requiring Infrastructure as a Service (IaaS) providers to notify the Commerce Department "when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."[37] The EO adds that U.S. IaaS providers would be prohibited from permitting foreign companies to resell their services or opening accounts for foreign persons unless the U.S. providers make similar disclosures.

The Treasury Department is also required to issue a report on best practices for financial institutions to manage AI-specific cybersecurity risks, and the Department of Homeland Security and Department of Defense are directed to study and report on how AI can be used in cyber defense.

8. Health and Biometric Privacy Litigation

Hospitals and other health-care businesses faced civil litigation pressure in 2023 over data breaches exposing patients' personal health information ("PHI"). For example, on March 13, 2023, a patient "Jane Doe" filed a class action lawsuit against Lehigh Valley Health Network ("LVHN") alleging that LVHN had failed to meet its duties under HIPAA to protect photographs of her

---

32 U.S. Department of Health and Human Services, *Resolution Agreements* (last updated Dec. 14, 2023), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

33 European Commission, *Adequacy Decision for the EU-US Data Privacy Framework* (July 10, 2023), https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

34 Data Privacy Framework Program, *Key Requirements for DPF Program Participating Organizations*, https://www.dataprivacyframework.gov/s/key-requirements.

35 *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 88 Fed. Reg. 75191 (Nov. 1, 2023).

36 *Id.* at 75193 (section 2(f)).

37 *Id.* at 75198 (section 4.2(c)(i)).

naked torso, as well as identity information such as her date of birth, social security number, and diagnosis details, from being leaked online by a ransomware gang.[38]

HIPAA obligations were also the subject of litigation over advertising tracking code, also known as tracking pixels, that are allegedly able to send PHI, including diagnoses and medical appointment details, to third parties, including for use in marketing efforts that target individuals with particular conditions and diagnoses.[39] The FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) have issued joint letters to approximately 130 hospital systems and telehealth providers alerting them to the risks of using such tracking technologies.[40]

Litigation under Illinois's Biometric Information Privacy Act ("BIPA") litigation continued in 2023, with the Illinois Supreme Court ruling that BIPA claims accrue on a per-incident basis when an employer uses fingerprint scans for employees to clock in without obtaining the employees' consent.[41] Employers may be subject to a wide range of BIPA claims, which can be brought as a private right of action under the statute, based on their reliance on biometric data for authentication of employee identity and attendance.[42]

9. Attorney-Client Privilege Found Not to Protect the Identity of Victims of Cyber Incidents at Law Firms

On January 10, 2023, the SEC filed suit against law firm Covington & Burling LLP, seeking a court order to obtain a list of clients affected by a cybersecurity breach at the firm in November 2020.[43] The SEC argued that it needed the client list to determine if the affected companies were in compliance with reporting regulations under the federal securities laws, while Covington asserted that the list of its clients' names was protected by the attorney-client privilege. Although the court ultimately ruled that Covington did not need to disclose the names of all clients whose information was believed to have been stolen from the firm, on July 24, 2023, Judge Amit Mehta ordered Covington to disclose the identities of seven public company clients that may have had material nonpublic information stolen in the incident.[44] Covington and the SEC agreed not to appeal, but one of the seven clients has been granted anonymity during the pendency of its appeal of the order.[45]

10. Continued GDPR Enforcement, Plus a New Swiss Data Privacy Law

European regulators and privacy advocates continued efforts to limit and regulate the use of personal data for marketing and advertising, prompting changes to business practices and models that will remain subject to scrutiny. Indeed, even after a social media company rolled out an ad-free subscription option in Europe in response to GDPR enforcement actions against it for

38 https://www.theregister.com/2023/03/15/cancer_lvhn_sues_hospital/?td=rt-3a.

39 *See, e.g.*, Compl., *Nienaber* v. *Overlake Hosp. Med. Ctr.*, No. 2:23-cv-1159 (W.D. Wash. Aug. 3, 2023).

40 Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies* (July 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

41 *Mosby* v. *Ingalls Memorial Hospital*, No. 129081, 2023 IL 129081 (Ill. Nov. 30, 2023).

42 John Wolak & William Martinez, *That's a Super-Sized Sack of Sliders: Illinois Supreme Court Finds White Castle Could Face Up to $17 Billion in Damages*, American Bar Association (May 15, 2023), https://www.americanbar.org/groups/business_law/resources/business-law-today/2023-may/illinois-supreme-court-finds-white-castle-could-face-up-to-17b-in-damages/.

43 Compl., *SEC* v. *Covington & Burling LLP*, No. 23-mc-2 (D.D.C. Jan. 10, 2023).

44 *SEC* v. *Covington & Burling, LLP*, No. 23-cv-2, 2023 WL 4706125 (D.D.C. July 24, 2023).

45 Andrew Goudward, *SEC, Covington End Legal Fight Over Client Names, But Dispute Isn't Over*, Reuters (Sept. 18, 2023), https://www.reuters.com/legal/legalindustry/sec-covington-end-legal-fight-over-client-names-dispute-isnt-over-2023-09-18/.

ad-tracking, privacy advocates vowed to challenge the new plan as an allegedly coercive "pay or okay" method to obtain ad-tracking consent.[46]

And in June, the French data privacy regulator CNIL fined online advertising company Criteo €40 million, alleging that the company had violated the GDPR by tracking consumers online and using their data for targeted advertising. The CNIL described Criteo's business focus as "behavioral retargeting"—delivering personalized advertisements to individual users by using cookie data to analyze the user's browsing habits. The CNIL found that the company did not obtain consent from consumers before using their data for behavioral retargeting. And even though Criteo's data did not include users' names, the CNIL found that the company had collected data accurate enough to re-identify some individuals.[47]

The revised Swiss Federal Act on Data Protection (revFADP), which passed in 2020, came into force on September 1, 2023, bringing Switzerland's regulation of data privacy into closer alignment with the EU GDPR. The law has a broad geographic scope, purporting to apply to any activity with an impact in Switzerland, as well as covering the storage by any entity of personal data on servers located in Switzerland. Covered entities that are engaged in large-scale processing activities that pose a high risk to data subjects are required to appoint a representative in Switzerland to act as a point of contact for Swiss data subjects.[48] Companies that have known for some time about the regulatory requirements and risks of processing personal data in the EU no longer have many of the benefits of a more flexible regime in Switzerland.

* * *

46 Natasha Lomas, *Meta to Offer Ad-Free Subscription in Europe in Bid to Keep Tracking Other Users*, TechCrunch (Oct. 30, 2023), https://techcrunch.com/2023/10/30/meta-ad-free-sub-eu/.

47 CNIL, *Personalised Advertising: CRITEO Fined EUR 40 Million* (June 22, 2023), https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million.

48 Andreas Matzler & Charlotte Mason, *Ready for the New Swiss Data Protection Law? Implications for Organizations Outside Switzerland*, Int'l Ass'n of Priv. Pros. (Aug. 17, 2023), https://iapp.org/news/a/revised-swiss-data-protection-law-soon-in-effect-with-new-scope-obligations-implications/.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Katherine Fang, Anita Y. Liu and Rosie Vail and staff attorney Emily B. Compton contributed to this Client Memorandum.