PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

PRIVACY LAW SECTION JOURNAL

PRIVACY LAW

INSIDE THIS ISSUE

VOLUME 1 2024

SECTION OFFICERS & EDITORIAL BOARD

OFFICERS:

CHAIR

Nicholas Ginger
San Francisco

VICE CHAIR

Hailun Ying
San Mateo

SECRETARY

Cody Venzke
Washington D.C.

TREASURER

Andrew Scott
Larkspur

IMMEDIATE PAST CHAIR

Sheri Porath Rockwell
Los Angeles

CLA BOARD REPRESENTATIVE:

Joshua de Larios-Heiman
San Francisco

EXECUTIVE COMMITTEE:

Taylor Bloom
Costa Mesa

Brett Cook
Fort Worth, TX

Christian Hammerl
Walnut Creek

Elaine Harwell
San Diego

Michael Hellbusch
Costa Mesa

Paul Lanois
Palo Alto

Steven Millendorf
San Diego

Jennifer L. Mitchell
Los Angeles

Hina Moheyuddin
Hollister

Jeewon Serrato
San Francisco

Robert Tookoian
Fresno

INTRODUCTION FROM THE PRIVACY LAW SECTION CHAIR

Written by Nicholas Ginger

It is my distinct pleasure to welcome you to the Privacy Law Section's first Journal. When our Section was formed several years ago, we set out a list of accomplishments we hoped to achieve. You are holding in your hands the end result of one of our more ambitious goals, a print publication that facilitates dialogue and thought leadership in the emerging area of Privacy law. And yet, our first publication could not be more timely. Since the inception of our Section, approximately twelve states have enacted comprehensive privacy laws, the U.S. and the E.U. have agreed on a major new data transfer program, reproductive health data became evidence for prosecutions in several states, there has been increased awareness of the detrimental effects of social media on teen mental health, dramatic developments in artificial intelligence have reinvigorated concerns over systematized biases, and yes, there was a major pandemic that pushed the social and work lives of millions of people online, exposing our data to countless malefactors. Clearly the need for Privacy professionals is at an all-time high.

As Chair, it is my privilege to speak on behalf of the Privacy Law Section, but make no mistake, the Section is buoyed by a tremendous group of attorneys and dedicated volunteers who share in their passion for the importance of Privacy law. The Section has accomplished much in its short existence. This past February, we held our first Annual Summit and by all accounts it was an amazing conference attended by practitioners and regulators alike. We established the Privacy Lawyer of the Year Award, recognizing those who have made outstanding contributions to the development of California privacy law. We publish regular privacy news updates and articles about the developments in California privacy and other privacy laws. Our legislative committee actively monitors proposed legislation and submits neutral comments on behalf of the CLA. We have also established an education committee that organizes MCLE programming. I encourage you to join us and help build out the Section for future generations of privacy lawyers. Doing so would make you part of one of the most inclusive, diverse, and rewarding communities of professionals that I have ever had the benefit of working with - the Privacy community.

We are only at the beginning.

Nick Ginger

Nicholas Ginger
Chair, Executive Committee

LETTER FROM THE EDITORS

AUTHORS

Jennifer L. Mitchell

Kewa Jiang

Robert Tookoian

We are thrilled to present to you a collection of commentary on today's most timely and impactful privacy issues from top esteemed experts in our field. In this inaugural print publication of the California Lawyer Association's Privacy Law Section, we ambitiously cover topics ranging from generative AI to consumer health data privacy to ad tech and privacy litigation trends. We have also included a comprehensive guide to building an international privacy compliance program, and an inspiring interview with Lydia F. de la Torre, one of the five members of the Board of the California Privacy Protection Agency (CPPA).

Established in 2020, the Privacy Law Section is the newest section within the California Lawyers Association. The mission of the Privacy Law Section is to bring together privacy practitioners working in diverse settings, to provide members with a range of unique educational opportunities, and to allow for an exchange of ideas and technical expertise. Our members include privacy attorneys working in practice settings ranging from private practice to in-house privacy and cybersecurity roles, as well as consumer privacy advocates, government regulators, and policy analysts at privacy think tanks.

We invite you to join our dynamic and accomplished group of privacy leaders in the Section's year ahead, which will undoubtedly be more exciting than the last. We also hope to see you in sunny Los Angeles at our Second Annual Privacy Summit from February 8-9, 2024.

We would like to thank all of our contributors, several of whom had to adjust their content mid-draft to keep in pace with the rapidly changing developments in our field. We are grateful for your insights and your leadership.

We hope that you enjoy.

Jennifer L. Mitchell
Executive Committee Member
Chair of Privacy Publications

Kewa Jiang
Vice-Chair of Privacy Publications

Robert Tookoian
Executive Committee Member
Vice-Chair of Privacy Publications

MCLE SELF-STUDY ARTICLE:

PRIVACY LAW ISSUES ASSOCIATED WITH DEVELOPING AND DEPLOYING GENERATIVE AI TOOLS

Written by Jonathan Tam*

The past couple of years have seen significant technological advancements in artificial intelligence ("**AI**") and legal developments applicable to organizations that develop and deploy (i.e., adopt and use) AI. This article outlines examples of developments related to privacy law and AI at the U.S. federal and California state level and examines at a high level some privacy issues that organizations should consider before developing or deploying generative AI ("**GenAI**") tools, which are a subset of AI technologies that generate new content in response to a user instruction or prompt.

EXAMPLES OF DEVELOPMENTS RELATED TO PRIVACY LAW AND AI AT THE FEDERAL AND CALIFORNIA STATE LEVEL

On October 30, 2023, President Biden issued the "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" ("**EO 14110**").[1] The order defines "AI" as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."[2] EO 14110 also defines "generative AI" as "the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content," and "synthetic content" as "information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI."[3]

As a side note, these definitions arguably do not cover all systems that many people would consider to be GenAI systems. For example, many people would consider chatbots and tools that can create text responses, images, audio clips or videos based on user prompts to constitute GenAI. But if such a tool can only be used to create artwork, summarize other works, or develop harmful materials such as misinformation, the tool arguably falls outside EO 14110's definition of "AI" because such output does not constitute "predictions, recommendations, or decisions". Another argument is that the definition of "AI" is too broad. If one interprets its elements expansively—for example, by construing the word "decision" to mean any algorithmic output—then the definition arguably covers any software that runs on a machine, was designed or used by a human, and generates algorithmic output. This side note is intended to suggest that the terms "AI" and "GenAI" are not easily defined and there may be competing theories on how they should be defined.

EO 14110 calls out the need for the Federal Government to protect Americans' privacy. The order pursues this

objective in various ways, including by: (i) ordering the Office of Management and Budget to develop guidance on how federal agencies should procure and process "commercially available information" in a privacy-protective way; (ii) promoting the adoption of "differential-privacy guarantees" so that datasets about groups of entities that an organization shares with another cannot easily be used to identify specific entities from that dataset; and (iii) ordering the creation of a government-funded body called the Research Coordination Network dedicated to advancing privacy research and developing privacy-enhancing technologies.[4]

On October 4, 2022, the White House issued the Blueprint for an AI Bill of Rights ("**Blueprint**"),[5] which sets forth five non-legally-binding principles intended to protect people from the harms of automated systems. One of these principles is centered on data privacy.[6] The Blueprint notes, among other things, that designers, developers and deployers of automated systems should: (i) set privacy defaults so that they conform with users' reasonable expectations; (ii) only collect personal information that is strictly necessary for the specific context; (iii) seek permission to process personal information where appropriate; (iv) provide privacy notices and consent requests in a plain language; (v) implement special protections for sensitive data; and (vi) avoid unchecked surveillance.

The Federal Trade Commission ("**FTC**") has also published various guidance documents focused on AI issues,[7] including one that describes GenAI as follows:[8]

> "Generative AI" is a category of AI that empowers machines to generate new content rather than simply analyze or manipulate existing data. By using models trained on vast amounts of data, generative AI can generate content—such as text, photos, audio, or video—that is sometimes indistinguishable from content crafted directly by humans. Large language models (LLMs), which power chatbots and other text-based AI tools, represent one common type of generative AI. Many generative AI models are developed using a multi-step process: a pre-training step, a fine-tuning step, and potential customization steps. These steps may all be performed by the same company, or each step may be performed by a different company.

The FTC has the authority to take privacy-related enforcement actions against companies, including under the Children's Online Privacy Protection Act and its regulations ("**COPPA**"), and Section 5 of the Federal Trade Commission Act ("**FTC Act**"), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC has warned that AI, including GenAI, can be used to engage in privacy infringements,[9] and published statements focused on the intersection of AI and biometric information.[10]

At the state level, California Governor Newsom published an executive order on GenAI on September 6, 2023.[11] The order requires, among other things, that a handful of state government agencies issue general guidelines for public sector procurement, uses and required trainings of GenAI that address applicable privacy risks. The order does not enumerate new privacy risks but refers to risks already outlined in the White House's Blueprint.[12]

On November 16, 2023, the California Bar's Board of Trustees approved Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law.[13] The guidance does not categorically prohibit lawyers from using AI, but identifies a number of ways in which lawyers' ethical and professional obligations apply to the use of GenAI. For example, the guidance reminds lawyers that GenAI raise privacy law issues and lawyers cannot counsel a client to engage in a violation of laws, or assist in any such violations, when using GenAI tools.[14]

On August 29, 2023, the California Privacy Protection Agency ("**CPPA**") published draft regulations regarding risk assessments.[15] By way of background, the California Consumer Privacy Act of 2018 ("**CCPA**"),[16] contemplates that businesses (i.e., entities that do business in California, determine the means and purposes of processing personal information and meet certain quantitative thresholds) must regularly submit risk assessments to the CPPA when they process California residents' personal information in ways that present significant risks to their privacy or security. The CPPA's draft regulations include a definition of "Artificial Intelligence" that is similar, but arguably broader than the definition in EO 14110.[17] It states, among other things, that businesses that process California residents' personal information to train such technologies automatically engage in processing activities that present significant risks to their privacy, thereby triggering duties to complete a risk assessment.[18] The draft regulations enumerate various elements that a risk assessment must incorporate, including the benefits resulting from the processing, the negative impacts to California residents' privacy associated with the processing, the planned safeguards to address the negative impacts, and whether the negative impacts, as mitigated by the planned safeguards, outweigh the benefits

resulting from the processing.[19] The CPPA's draft risk assessment regulations may undergo further revision prior to finalization.

New legal developments governing the privacy dimensions of AI continue to unfold at a rapid rate, and privacy practitioners should continue to monitor the space for new laws, regulations, cases and regulatory guidance materials.

PRIVACY ISSUES COMMONLY RAISED WHEN DEVELOPING OR DEPLOYING GENAI

As discussed above, companies that develop GenAI tools typically procure large sets of raw data, modify the data to produce training data (such as by deleting duplicate data), feed the training data into an AI model to train it to recognize patterns, and fine-tune the AI model until it meets certain standards, such as to ensure the output is sufficiently responsive, intelligible and accurate. The datasets that developers procure and process to train GenAI tools, and the output that the tools generate, may contain personal information. In addition, companies that deploy GenAI tools may include personal information in the prompts or other datasets that they want the tools to take into account when generating output.

A number of privacy compliance considerations and requirements may apply to developers of GenAI tools, such that they may wish to:

- Consider whether and the extent to which the CCPA's exemption for "publicly available information" may apply to the developer's proposed processing activities, such as the procurement of data for training purposes;[20]
- Provide notices (such as notices at collection, which must be provided at or before the point at which a business subject to the CCPA collects a California resident's personal information, unless an exception applies) and obtain consents (which a business subject to the CCPA must do in certain situations, such as before selling the personal information of a minor under the age of 16, unless an exception applies), as required or appropriate, to individuals whose personal information is collected and used to train the model or operate the tool, or whose personal information may be included in the tool's output;[21]
- Avoid retaining personal information for longer than reasonably necessary to discharge the disclosed purposes for which it was collected, which may require deleting training data once it is no longer reasonably necessary to train the model;[22]
- Comply with the CCPA's necessity, proportionality and purpose limitation requirements, which may require an overall examination of what types of data and processing are necessary and proportional to the development of the AI model;[23]
- Determine whether the developer sells personal information, as the CCPA defines "sell",[24] in connection with developing or operating the model (which may be the case if a third party can use personal information from the developer for its own purposes, even if the third party did not pay for the information) and, if there is selling and the CCPA applies, comply with various related obligations including to obtain opt-in consent for minors under the age of 16 and giving other individuals the ability to opt-out of sales;[25]
- Evaluate whether the developer uses California residents' "sensitive personal information", as the CCPA defines this term,[26] for purposes not subject to an exception or exemption and, if so, comply with requirements related to allowing them to opt out of such uses of their sensitive personal information—note that the CCPA exceptions include to perform, improve, upgrade or enhance services, which may apply to training an AI model;[27]
- Honor requests from California residents to know, delete or correct their personal information, which may oblige the developer to maintain granular control over how the tool generates output about a particular individual (for example, the tool may need to "relearn" facts about an individual if its prior configuration generated incorrect information about the individual and the individual submitted a correction request);[28] and
- Implement security measures as required by applicable laws to protect personal information from unauthorized or illegal processing, which may include red-teaming (i.e., intentionally acting as an adverse party to test the vulnerabilities of the system) the model to minimize the risks of it revealing personal information about individuals unless there is a lawful basis to do so.[29]

A number of privacy compliance considerations and requirements may also apply to deployers of GenAI tools, such that they may wish to:

- Consider whether it is permitted to disclose personal information to developers and operators of GenAI tools, such as in prompts, or if it is required to issue any notices or obtain any consents before doing so;[30]
- Determine whether it is necessary to conduct a risk assessment, privacy impact assessment or similar assessment to evaluate the risks versus the benefits of deploying the GenAI tool;[31]
- Enter into appropriate data processing or protection clauses with the provider of the tool, depending on whether the provider serves as the deployer's "service provider" or "contractor", or as a "third party", as the CCPA defines these terms;[32]
- Evaluate whether the provider's data security measures are adequate;[33]
- Implement policies, protocols and training to ensure that personnel who use the tool do so only in compliance with applicable legal obligations, which may include compliance with necessity, proportionality and purpose limitation requirements;[34] and
- Ensure that any output generated by the tool is covered by the deployer's protocols and policies related to honoring California residents' CCPA rights, including access, deletion, correct and opt-out rights (e.g., prompts and outputs containing an individual's personal information will be deleted upon request unless an exception applies).[35]

The above considerations are some examples of privacy-related points that companies may wish to take into account when developing, providing and deploying GenAI tools. Issues outside of privacy may also apply to the development and deployment of GenAI, including under intellectual property, anti-discrimination, product safety, contract, tort and other laws.

ENDNOTES

* Jonathan Tam is a partner in Baker McKenzie's San Francisco office specializing in privacy, cybersecurity, consumer protection and tech transactions. He is dually licensed in Canada and the U.S. and has helped numerous companies with implementing privacy and security compliance programs, leading data incident responses, negotiating data processing and other agreements, and representing companies in the context of data-related regulatory investigations. Jonathan is incoming Chair of the Executive Committee of the Cybersecurity & Privacy Section of the San Francisco Bar Association, and CIPP/C and CIPP/US certified. He regularly publishes and speaks on privacy and tech topics. He is a graduate of the University of Toronto Faculty of Law and Harvard College.

1. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." White House. October 30, 2023. Available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
2. *Ibid*., at Subsection 3(b).
3. *Ibid*., at Subsections 3(p) and (ee).
4. *Ibid*., at Section 9.
5. "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." October 3, 2023. The White House Office of Science and Technology Policy. Available at: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
6. The others are: (i) safe and effective systems; (ii) algorithmic discrimination protections; (iii) notice and explanation; and (iv) human alternatives, consideration and fallback.
7. See, e.g., "Consumers are Voicing Concerns about AI". Federal Trade Commission. October 3, 2023. Available at: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/10/consumers-are-voicing-concerns-about-ai.
8. "Generative AI Raises Competition Concerns". Federal Trade Commission. June 29, 2023. Available at: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.
9. "FTC Authorizes Compulsory Process for AI-related Products and Services". Federal Trade Commission. November 21, 2023. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-authorizes-compulsory-process-ai-related-products-services.

10. See, e.g., "Preventing the Harms of AI-enabled Voice Cloning". Federal Trade Commission. November 16, 2023. Available at: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/preventing-harms-ai-enabled-voice-cloning.

11. Executive Order N-12-23. Office of Governor Gavin Newsom. September 6, 2023. Available at: https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12-_-GGN-Signed.pdf.

12. *Ibid*., at Subsection 3(a).

13. "Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law". The State Bar of California. November 16, 2023. Available at: https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf.

14. *Ibid*., at page 3.

15. "Draft Risk Assessment Regulations for California Privacy Protection Agency September 8, 2023 Board Meeting" ("Draft Risk Assessment Regulations"). California Privacy Protection Agency. August 29, 2023. Available at: https://cppa.ca.gov/meetings/materials/20230908item8part2.pdf.

16. As amended by the California Privacy Rights Act of 2020.

17. The draft regulations defined "Artificial Intelligence" as "an engineered or machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments. Artificial intelligence includes generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial or speech recognition or detection technology."

18. Draft Risk Assessment Regulations at page 4.

19. *Ibid*., at pages 6-11.

20. The CCPA excludes "publicly available information" from the scope of protected personal information, and defines publicly available information as "information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer [i.e., the California resident who is the subject of the information] or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge." Cal. Civ. Code § 1798.140(v)(2).

21. See, e.g., Cal. Civ. Code §§ 1798.100, 1798.120(c) and 1798.125.

22. See, e.g., *ibid* at § 1798.100(a)(3).

23. See, e.g., *ibid* at § 1798.100(c).

24. The CCPA defines "selling" to mean the disclosure of personal information for monetary or other valuable consideration unless an exception applies. Cal. Civ. Code § 1798.140(ad).

25. See, e.g., *ibid* at § 1798.120.

26. The CCPA defines "sensitive personal information" to include certain categories of personal information including a California resident's racial or ethnic origin, genetic data, passport number, and other categories. The definition was recently amended to include citizenship and immigration status as well (AB 947). For the full definition of "sensitive personal information", see Cal. Civ. Code § 1798.140(ae).

27. See, e.g., *ibid* at § 1798.121.

28. See, e.g., *ibid* at § 1798.130.

29. See, e.g., *ibid* at § 1798.100(e).

30. See, e.g., Cal. Civ. Code §§ 1798.100, 1798.120(c) and 1798.125.

31. See, e.g., *ibid* at § 1798.185(15)(B) and supra at note 14.

32. See, e.g., *ibid* at §§ 1798.100(d) and 1798.145(j), (ag) and (ai).

33. See, e.g., *ibid* at § 1798.100(e).

34. See, e.g., *ibid* at § 1798.100(c).

35. See, e.g., *ibid* at § 1798.130.

CHAT BOTS AND COOKIES AND PIXELS, OH MY!

Written by Jennifer M. Oliver*

While more U.S. states are introducing and enacting new privacy legislation, plaintiffs are increasingly turning to laws that have been on the books for 50 or more years to pursue individual and class action privacy litigation against companies using software vendors to analyze web traffic or ad tracking technology, such as Meta Platforms Inc.'s Pixel tracking tool.

These session replay software, third party chat features, and pixels are commonplace on consumer facing websites. But now plaintiffs are alleging that when these tools capture browsing data and share it with third parties, for example software providers and social media companies, the companies utilizing them violate state wiretap acts—notably in Florida, Illinois, Pennsylvania, and, perhaps most commonly, California. Several district court decisions allowing these claims to proceed past the pleading stage on a theory of aiding and abetting against a website owner, allowing a third party to facilitate its chat function, has emboldened class action attorneys in California.[1]

California courts have seen a significant uptick in putative class actions under Section 631 of California's "wiretapping" statute.[2] There, plaintiffs claim that where a third-party provider of chat, session replay, or Pixel functionality has simultaneous, real-time access to website "communications," without the website user's knowledge or consent, the website operator is "aiding and abetting" the third-party vendor's Section 631 violation.

And a review of class actions on the public dockets reveals only the tip of the iceberg: there are many more individual private arbitrations being filed against companies with arbitration clauses contained in their website term and conditions as well. Because a putative plaintiff need only visit a public facing website to bring a claim, it is relatively easy for plaintiffs' firms to amass a large number of individual arbitration claimants. While may companies believe that mandatory arbitration clauses and class action waivers are protecting them from costly class action litigation in court, when dozens or even hundreds of individual claims are filed, the cost of filing fees alone can compound and exceed in court litigation. For example, cases with only a single $5,000 violation, represent a significant percentage of the value of each individual claim.

CHAT AND SESSION-REPLAY CASES

Chat and session replay software were the first wave of suits in California courts. Chat bots are familiar to most internet users, many consumer-facing website use a third-party chat provider to enable the feature on their site and allows consumers to chat in real time with consumer service representatives. But where a third party has access to those chants, and consumers do not consent to that access, plaintiffs will allege that a wiretap has occurred.

Session-replay software allows website operators to record mouse movements, keystrokes, and search information inputted into websites, as well as pages and content viewed. In this way, session-replay software allows a website operator to "replay" a visitor's journey on a website or within a mobile or web application. Rather than focusing on user activity after leaving a particular website, session-replay software focuses on how a user interacts with a specific website. Marketing departments use this data to better understand the users' experiences and gain visibility into the bugs, errors, or confusing moments they may encounter.

Again, if the session replay vendor has access to the session repay data, plaintiffs will allege that a wiretap has occurred.

One key consideration is whether any involved session replay vendor or service provider is limited by agreement (or otherwise) to using the website activity data only to analyze the website's functionality for the company's benefit, rather than for the provider's own independent purposes. There is at least some good news for website operators on this front: at least one court has held that session-replay technology cannot form the basis of a California Invasion of Privacy Act (CIPA) claim because a service provider does not use the data for its own purposes; it is an extension of the website provider, and a party cannot "tap its own wire."[3] However, even where there are such terms favorable to defendants, they can be challenging to introduce at the motion to dismiss stage where defendants are limited to the four corners of the pleadings.

But, on the other hand, in *Saleh* v. *Nike, Inc.*,[4] the court found that where a third-party software provider has simultaneous, real-time access to a customer's website communications, without the customer's consent, that third-party vendor cannot avail itself of the rule that parties to a communication cannot also be wiretappers under CIPA. Although that logic would seem to implicate the vendor as the "wiretapper" and not the website operator, the *Saleh* court went on to find that the website operator "aided and abetted" the violation, creating a real risk for website operators embedding chat software to communicate with California customers.[5]

META PIXEL CASES

Perhaps the most popular brand of wiretapping cases as of late are those involving use of the Meta Pixel tracking tool. The Meta Pixel is free code, courtesy of Meta, that can be used on a company's website to track user activity. Used by companies for targeted advertising, the code transmits certain information about a user's interaction with a website that uses the Pixel to Meta, including the HTTP headers, pixel-specific data (Pixel ID and cookie), and other information based on company configuration.

Here, plaintiffs allege that the Pixel shares browsing data with Facebook and Facebook is a third party wiretapper collecting this data for its own gain. This distinguishes these cases from the chat and wiretapping cases because, in those cases, it is easier to argue that the software provider is a vendor acting on behalf of the defendant and not really a third party wiretapping any sort of communication for its own purposes or gain.

Perhaps the most watched Meta Pixel privacy lawsuit is In re Meta Pixel Healthcare Litigation,[6] a putative class action against Meta for allowing sensitive health data to be sent to Meta from healthcare providers' websites, including patient portals, without consent. In September of 2023 the federal judge in that case denied Meta's motion to dismiss many of its claims, including wiretap allegations.

The November 1, 2023 approval of a $13,000,000 class-wide in *Hodges* v. *GoodRX Holdings, Inc.*,[7] is also notable. There plaintiffs alleged that use of various pixels and SDKs (software development kits) on GoodRX's website violated state and federal wiretapping statutes, consumer protection laws, and common law privacy rights by intercepting user data and sharing it with vendors without users' consent.

VIDEO PRIVACY PROTECTION ACT OF 1988 (VPPA)

In cases where the defendant uses on demand streaming content on their website and viewership data is shared with Facebook, plaintiffs will also allege a violation of the Video Privacy Protection Act of 1988 (VPPA) by use of the Meta Pixel. The VPPA is a federal law that prohibits videotape service providers from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider . . ." Under the VPPA, "personally identifiable information" is defined as "includ[ing] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." According to the VPPA, a "video services provider" is defined as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials . . ." which has been interpreted in court cases as extending to websites streaming online video. States followed by enacting their own versions of the federal law, some of which expanded protected materials.

These lawsuits allege that companies that stream online video content on their websites and use the Meta Pixel violated the VPPA by transmitting personally identifiable information about a user to Meta. Earlier lawsuits filed focused on companies whose business significantly involved video content (e.g., Patreon).

Some courts have dismissed these VPPA Meta Pixel cases already while others have allowed them to survive the motion to dismiss stage. *Ambrose* v. *Boston Globe Media Partners LLC*, a case in federal court in the District of Massachusetts, was one

of the earliest VPPA Meta Pixel class action lawsuits filed. In September 2022, the case survived the defendant's motion to dismiss as the judge ruled that the plaintiff had stated a viable claim, although the court may later determine that the website does not transfer the plaintiff's personally identifiable information to Meta as alleged.

Martin v. *Meredith Corp.* was a Meta Pixel case filed in the Southern District of New York alleging the media company, which operates various websites including People.com, violated the VPPA. The court dismissed the case on the grounds that the "version of the Facebook Pixel used on People.com sends only the Facebook ID and the name of the webpage that a user accessed" and thus it did not send personally identifiable information under the definition of the statute (i.e., information about whether an individual "requested or obtained specific video materials or services.")

COMMON LAW AND OTHER STATUTORY CLAIMS

In many of these cases, plaintiffs are also often asserting common law invasion of privacy violation claims. The cases generally assert that plaintiffs had a legitimate expectation of privacy regarding their private information, an expectation that the defendant would not disclose this information to third parties without their consent.

Other statutory claims have started to appear in these complaints as well, almost always secondary to a CIPA claim. For example, in some cases plaintiffs allege violation of Cal. Pen. Code 638.51, which regulates the use of a "pen register" or "trap and track device." Other complaints allege violation of the California Consumer Data Access and Fraud Act ("CDAFA"), Cal. Pen. Code § 502, which is "an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose."[8]

In the healthcare context, these cases also typically allege violation of the California Medical Information Act, which states that "[a]ny provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to . . . remedies and penalties . . ."[9]

DEFENSES

Defendants have numerous defenses at their disposal when attempting to defeat these claims. For example, defendants often argue that the plaintiff lacks standing because plaintiff visited the website as a purported "tester," or ignored the landing page banner notifying users of the involved technologies and/or linking to the online privacy policy. Article II Standing can also be leveraged, but in cases where plaintiffs filed in state court and defendants choose to remove to federal court, defendants will waive the right to that defense.

Companies often argue that they are exempt from liability as a party to the communication.[10] This argument is useful in session replay cases in which the session replay technology merely recorded and stored users' interactions with the site. It is less helpful in cases where plaintiffs can plausibly allege that a third party used the collected data for its own means.

To form a cause of action under Section 631(a), a communication must be intercepted "in transit" between the user's device and the website server. Because online communications are nearly instantaneous, defendants can argue that the challenged access to the communication did not occur "in transit." However not all courts have found this compelling.[11]

Intent can be another useful defense for defendants in these cases; under CIPA § 631 a plaintiff must allege that a defendant "*intentionally* tap[ped] . . . any . . . wire, line, cable, or instrument" to state a claim under the first prong, or that defendant "*willfully* . . . read[], or attempt[ed] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit" to state a claim under the second prong.[12]

Also, Section 631(a) only prohibits the interception of the "contents" of communications. Courts have construed "contents" as limited to information constituting the intended message, as opposed to "record" information, such as keystrokes, mouse movements, and similar interactions typically stored via session replay technology. In re iPhone Application Litig., "'[C]ontents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication."[13]

And finally, defendants without significant California presence should be sure to assert personal jurisdiction defenses and may also wish to avail themselves of caselaw finding that the California Penal Code does not apply extraterritorially.[14]

MITIGATION

Mitigating the risk of these claims can be straightforward as long as there is an appetite for additional safeguards and the mitigating measures are implemented correctly. For example, explicit consent is a complete bar to these claims. In some cases, defendants can argue content, especially, for example, where plaintiffs agreed to Meta's terms and conditions and enabled cookies to allow Meta to collect their data.

Defendants will argue that "consent may be express or may be implied in fact from the surrounding circumstances indicating that the party to the call knowingly agreed to the surveillance."[15] "[A] party's awareness that he or she is being recorded may establish that the party impliedly consented to the recording."[16] But often plaintiffs will argue that these consents were not explicit enough or did not exist at all.

Forcing consumers to select their cookie preferences by affirmatively clicking "accept cookies," "decline all non-essential cookies," or "select cookies" as part of a well-worded cookie disclosure banner at the outset of a browsing session can mitigate this risk. Consumers should not be allowed to bypass the cookie banner without making a selection, and any pixels or software should not be allowed to fire until a selection is affirmatively made. However, it is important to consult with counsel to ensure that the disclosure is clear and that the user's instructions are honored lest the company can find itself in an even worse position for making an inadvertent misrepresentation regarding collection of data.

CONCLUSION

These cases show no signs of slowing down soon, and private plaintiffs aren't the only adversary to fear. The FTC has also pursued cases against companies in certain sectors for using these technologies without proper consumer consent.[17] While the law may ultimately develop in defendants' favor, companies should consider mitigating risk now.

ENDNOTES

* An experienced commercial litigator, Jennifer Oliver focuses her practice on complex litigation, with a specialty in website and privacy matters, defending consumer class actions, and consumer law compliance counseling. Jennifer has played active roles in several high-profile jury trials, serving as lead counsel in complex mediations, and arguing before courts at both the trial and appellate levels. She especially enjoys assisting her clients in navigating and avoiding consumer and privacy litigation.

1. *See*, e.g., *Augustine* v. *Lenovo* (United States), Inc., No. 22-cv-2027-L-AHG,2023 U.S. Dist. LEXIS 134595(S.D. CA, August 2, 2023); *Yockey* v. *Salesforce, Inc.*, No. 22-cv-09067-JST, 2023 U.S. Dist. LEXIS 150262 (N.D. CA, August 25, 2023); *Wright* v. *Ulta Salon*, No. 22-cv-1954-BAS-BLM,2023 U.S. Dist. LEXIS 159774 (S.D. CA, September 8, 2023)
2. California Invasion of Privacy Act (CIPA), California Penal Code Sections 630 et seq
3. *See*, e.g., *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 831 (N.D. Cal. 2021).
4. 562 F. Supp. 3d 503 (C.D. Cal. 2021).
5. *Id*. at 520-21.
6. Case No. 3:22-cv-3580-WHO-VKD (N.D Cal. 2023).
7. Case No. 1:23-cv-24128-BB (S.D Fla. 2023).
8. *Custom Packaging Supply, Inc. v. Phillips*, Case No. 2:15-CV-04584-ODW-AGR, 2015 WL 8334793, at *4 (C.D. Cal. Dec. 7, 2015).
9. Cal. Civ. Code § 56.101.
10. *See*, e.g., *Graham* v. *Noom, Inc.*, 533 F. Supp. 823, 829 (N.D. Cal. 2021).
11. *See*, e.g., *Wright* v. *Ulta Salon*, No. 22-cv-1954-BAS-BLM,2023 U.S. Dist. LEXIS 159774 (S.D. Cal. Sept. 8, 2023).
12. Cal. Pen. Code § 631 (emphasis added).
13. 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012); *See* also, In re Zynga Privacy Litig., 750 F. 3d 1098, 1107 (9th Cir. 2014).
14. *M Seven Sys. Ltd.* v. *Leap Wireless Int'l Inc.*, 2013 WL 12072526, at *3 (S.D. Cal. June 26, 2013); *Hammerling* v. *Google LLC*, No. 21-cv-09004-CRB, 2022 WL 17365255, at *11 (N.D. Cal. Dec. 1, 2022) (dismissing plaintiff's CIPA claim because plaintiff failed to allege that the data in question was intercepted in California).
15. *Nei Contracting & Eng'g, Inc.* v. *Hanson Aggregates Pac. Sw., Inc.*, No. 12-CV-01685-BAS (JLB), 2016 WL 4886933, at *3 (S.D. Cal. Sept. 15, 2016) (quoting *United States* v. *Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996)).
16. *Moledina* v. *Marriott Int'l, Inc.*, No. 2:22-cv-03059-SPGJPR, 2022 WL 16630276, at *7 (C.D. Cal. Oct. 17, 2022).
17. *See*, e.g., In the Matter of BetterHelp ($7.8 million settlement for partial refunds to customers); *United States* v. *GoodRx* ($1.5 million settlement and behavioral remedies).

THE WASHINGTON MY HEALTH MY DATA ACT: NOT JUST WASHINGTON (OR HEALTH)

Written by Mike Hintze*

Over the past several years, we've become accustomed to a rapid pace of change in the privacy law landscape—particularly at the U.S. state level. While there have been state privacy laws on the books for decades, the current era of seemingly weekly developments in state privacy law kicked off in 2018 with the adoption of the original California Consumer Privacy Act (CCPA). Since then, more than a dozen other states have enacted other comprehensive privacy laws, typically with broad similarities between them, but with enough significant differences to keep things interesting. Further amendments and/or rulemaking related to those laws creates what feels like a constantly moving target that is extremely challenging for those seeking to track, reconcile, and comply with them.

Earlier this year, a major development in Washington State further complicated this growing patchwork of state privacy laws. The passage of the Washington My Health My Data Act (MHMDA) is easily the most significant development in privacy law of 2023 and may be ***the most consequential privacy legislation enacted since the original CCPA***.

The Act purports to be focused on filling a gap by protecting health data not covered by HIPAA, the federal law that protects the privacy and security health data handled by hospitals, health care providers, and other enumerated "covered entities." But the Act is *very* different from HIPAA, and it does far more than just filling gaps.

Further, the Act is extremely broad in terms of the types of data covered and the entities that are subject to it. As a result, many companies (and nonprofits) that don't think of themselves as handling health data are surprised when they learn that they may be subject to the Act's obligations.

Those obligations are extensive, in several cases going well beyond what we have seen with any other privacy law. The sweeping scope and extreme substantive obligations, combined with vague terms and a private right of action, make this Act extraordinarily challenging and risky for a very wide range of organizations.

This Act is a privacy law for which perfect, risk-free compliance may be impossible. As entities that are potentially covered by the Act prepare for the March 31, 2024, effective date (June 30 for small businesses), they will need to carefully consider those risks as they determine and prioritize their compliance steps and investments.

PRIVATE RIGHT OF ACTION

In addition to Attorney General enforcement, the Act includes a private right or action, enforceable as a violation of the Washington Consumer Protection Act. The presence of a private right of action is significant, particularly in light of the Act's vague and open-ended language and near-impossible compliance standards.

Nevertheless, it is important to note that the Washington Consumer Protection Act does not include statutory damages, and to recover actual damages, a plaintiff needs to show both causation and an injury to the plaintiff's "business or property." However, the plaintiffs' bar is nothing if not creative and aggressive, and it is highly likely we will see a wave of costly and disruptive lawsuits. It remains to be seen whether Washington courts will start interpreting the "injury" requirement more permissively in light of the legislative intent behind My Health My Data Act.

In the meantime, companies will have to take this possibility into account in determining their compliance strategies to mitigate the risk of litigation and nuisance claims.

THE SCOPE OF THE ACT IS SWEEPING

The Act's definition of "consumer health data" can be interpreted to capture virtually any type or category of personal data about health, wellness, nutrition, fitness, or related topics–or that is used to infer such information. To give just one example, the definition includes "data that identifies a consumer seeking health care services." Health care services means "any service provided to a person to assess, measure, improve, or learn about a person's health." One could argue that a wide range of data processed by search engines, grocery stores and other retailers, gyms, advertisers, and any number of other businesses could fall into this sweeping scope. There are also several other parts of the definition that are similarly broad and open-ended.

There are a few narrow exceptions, primarily for data used for certain approved peer-reviewed research in the public interest, deidentified data (if all the requirements for deidentification are met), and certain publicly available data. There are also exceptions for data that is subject to enumerated privacy laws, most notably HIPAA, GLBA, FCRA, and FERPA.

The Act also captures a wide range of entities. It includes any entity (including nonprofits) doing business in Washington or that provides products or services that are targeted to consumers in Washington. An FAQ on the Act published by the Office of the Attorney General suggests that "targeted" can mean merely being available in Washington. As such, in the absence of geo-blocking, it could capture a wide range of entities with little or no actual connection to Washington.

Likewise, the scope of consumers whose data is subject to the law is expansive—potentially global. Because of some odd and non-obvious definitions, the Act captures data about consumers who have no meaningful connection to Washington at all. The only connection need be that the data about them is merely processed in Washington. It is worth noting that some of the largest global cloud service providers are headquartered in Washington, with significant data center footprints in Washington. Thus, a huge amount of data about consumers located outside of Washington is potentially processed in Washington. In light of the private right of action, this factor can dramatically affect the size of a potential class.

KEY ASPECTS OF THE WASHINGTON MY HEALTH MY DATA ACT

Designed to protect the privacy of health data not covered by HIPAA, but is much broader.

Covers a very wide (and ill defined) range of personal data, entities, and consumers.

Opt-in consent for any data processing beyond what is necessary to provide a consumer-requested product or service.

Extremely onerous authorization requirement for data "sales".

Data subject rights that go further than any other existing law.

Unique notice requirements that seem to require a separate (and redundant) privacy notices.

A prohibition on geofencing around any facility that provides any (very broadly defined) "health care services".

A private right of action, in addition to AG enforcement.

THE SUBSTANTIVE OBLIGATIONS OF THE ACT ARE EXTREME

The Act requires ***opt-in, GDPR-level consent for any collection, use, disclosure, or other processing of consumer health data beyond what is necessary to provide a consumer-requested product or service***. There is also a requirement

for a *separate* opt-in consent for any "sharing" of consumer health data beyond what is required for a consumer-requested product or service—including any sharing with corporate affiliates. Note that "sharing" here has a normal English meaning of the word—not the odd advertising-specific definition found in the CCPA. Such consents cannot be inferred, bundled with other consents, obtained as part of a terms of use or other agreement, or obtained via deceptive design.

There is an even more onerous "authorization" requirement for data "sales." Here, "sale" is defined in the way it is defined under the CCPA, which has been interpreted to include a wide range of data transfers—including nearly all third-party online targeted advertising. There is no reason to think that it will be interpreted any more narrowly here. The authorization requirement is extremely onerous, requiring a written and signed document including specific details of the data to be sold, the selling and purchasing parties, the use of the data by the purchaser, and several additional terms. The authorization lasts for only one year and is revocable by the consumer at any time. These requirements and limitations create such burden that it is unlikely many companies will even attempt to seek an authorization to sell, resulting in a *de facto* prohibition on most activities that could constitute a "sale" including much third-party targeted advertising.

Data subject rights include a right to know / right of access similar to that in CCPA and other laws. But the access right also includes a right to receive a list of all third parties and affiliates with which consumer health data has been shared, along with online contact information for each, which will likely require entities to create new processes to track, compile, and provide this information.

The deletion right is sweeping and goes well beyond what is required by any other privacy law on the planet. Specifically, the deletion right in the Act ***lacks the common exceptions found in every other privacy law*** that gives consumers a right to delete personal data. There is not even an exception for situations where retention of the data is required for compliance with law. This will put companies in an impossible position of determining which law they must violate when a consumer makes a deletion request.

The deletion right also includes a passthrough requirement to send a notification of the consumer's request to all processors, affiliates, and third parties with which the consumer health data has been shared. And those processors, affiliates, and third parties have an absolute obligation to also delete the data (which goes much further than the similar passthrough notification in the CCPA).

The Act includes a notice obligation which requires the posting of a "Consumer Health Data Privacy Policy." This notice must contain a list of enumerated disclosures, most of which will be redundant of the organization's general privacy statement. One aspect that goes beyond what other privacy laws require is that the notice must include a list of specific affiliates with which consumer health data is shared. There is nothing in the Act that indicates it can be combined with the organization's general statement. This could be interpreted to mean there must be a separate notice even if that is largely redundant of existing privacy notices. And with the requirement to include a link to the Consumer Health Data Privacy Policy from apps and every page on the entity's website(s), the number of separate privacy links that may be required by different privacy laws continues to increase.

The Act includes a geofencing prohibition around any facility that provides "in-person health care services" where the geofence is used to (1) identify or track consumers seeking health care services, (2) collect consumer health data, or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services. As already noted, the definition of "consumer health data" is broad such that it potentially includes virtually any personal data. Likewise, the definition of "health care services" is broad and includes any services "to assess, measure, improve, or learn about a person's mental or physical health."

As such, ***the prohibition on geofencing could apply to a very wide range of businesses and common business activities***. For example, given such a broad definition, a grocery store that has in-store signage with nutrition tips could be seen as providing "in-person health care services." So, if that grocery store uses a geofence to offer coupons through its app when a consumer enters the store, it could, depending on the facts, be seen as violating this prohibition. This is an absolute prohibition—there is no provision allowing the business to obtain consent from the consumer for such activity.

There are other requirements that are somewhat less noteworthy in that they more or less align with requirements found in other privacy laws that most entities must also comply with. Nevertheless, entities that may be subject to the Act should review all the substantive obligations to ensure they have considered and addressed how they will comply.

CONCLUSION

As with any new law, there are number of unknowns about how this Act will be interpreted and enforced. However that uncertainty is even greater here as the Act breaks new ground by diverging dramatically from any other privacy law on the books, including adding new obligations that go beyond what any other privacy law requires and key definitions and terms that are ambiguous as to scope and requirements.

We will certainly learn more in the coming year as the Attorney General begins enforcement and plaintiffs bring cases. But in the meantime, companies and other entities subject to the law will need to make difficult decisions and investments in compliance.

In light of the uncertainties, there are a number of compliance options and strategies that entities may consider for this Act. Each entity will need to review the law and its data practices and put in place a plan based on its own assessment of risk, taking into account the nature of the data it processes, how it uses and shares it, the impact different compliance options will have on its operations and business objectives, its overall risk tolerance, and many other factors.

ENDNOTE

* Mike Hintze is a partner at Hintze Law PLLC, a part-time instructor at the University of Washington School of Law, and a recognized leader in privacy and data protection law, policy, and strategy. You can read more of his writing on the Washington My Health My Data Act on the Hintze Law website at https://hintzelaw.com/MHMDA.

SPOTLIGHT ON PROFESSOR LYDIA DE LA TORRE, CALIFORNIA PRIVACY PROTECTION AGENCY BOARD MEMBER

Written by Jennifer L. Mitchell*


Profesor Lydia de le Torre

Between Professor Lydia de le Torre's roles as a Board Member of the California Privacy Protection Agency (CPPA), the Founder of Golden Data Law, and a law school professor teaching novel courses on artificial intelligence (A.I.), there is no doubt that Prof. de la Torre is one of California's most influential privacy lawyers.

Prof. de la Torre was appointed to the CPPA Board by the California Senate President pro Tempore Toni G. Atkins in March 2021 and served on the Advisory Board of Californians for Consumer Privacy during the Prop 24 ballot campaign. She is an affiliated researcher at the Center for Data Science and Artificial Intelligence Research (CeDAR) and teaches privacy, data protection, and AI courses at UC Davis Law and U.C. Law San Francisco (formerly U.C. Hastings). Prof. de la Torre is the founding partner of the teaching law firm Golden Data Law (GDL). GDL serves clients in the not-for-profit sector, and its mission is to mentor a diverse and inclusive group of law students and recent grads so that they can grow into solid ethical professionals. Prior to her appointment, Prof. de la Torre served as an of-counsel to Squire Patton Boggs and had in-house counsel roles at several multinational organizations. Prof. de la Torre is an international expert in data protection issues and the European Union's approach to regulating data and A.I. in particular.

I had a chance to catch up with Prof. de la Torre to learn more about her distinguished career path, her background in comparative law, and her views on the future of privacy and the profession.

JENNIFER: Thank you for your history of supporting the California Lawyers Association (CLA), and we appreciate you taking the time to share your insights with us. Could you tell us about your background, starting as a European-trained lawyer, and how you ended up specializing in privacy?

PROF. DE LA TORRE: I was born and raised in Spain and completed my law studies at the Complutense Facultad de Derecho in Madrid, from which I graduated in 1995. I wanted to work for the Arthur Andersen organization, which in Spain at the time had three branches: an accounting/auditing branch (which collapsed in 2001 after the Enron scandal), a consulting arm (which later became Accenture), and a law firm (Arthur Andersen Asesores Legales y Tributarios.) With that purpose in mind, I enrolled in an LLM program in taxation offered by Arthur Andersen and joined the Arthur Andersen law firm arm in 1996. Shortly after I joined, the firm merged with the leading local law firm, Garrigues, the name under which the firm still exists today. Because of the merger, the corporate practice grew significantly. I was able to move from the practice of tax law to corporate practice by working under Pablo Olabarry, a now-retired partner who is one of the most brilliant corporate attorneys with whom I have had the privilege to work with and who, incidentally,

was one of my teachers during the LLM program. Since I was highly interested in emerging technologies, I raised my hand, so to speak, to be called upon to do any corporate or transactional work that was connected to them.

One of the laws affecting emerging technologies that were in effect at the time was the LORTAD (Ley Orgánica 4/92 de Regulación del Tratamiento Automatizado de Datos), enacted in 1992. This Spanish law pre-dates the EU privacy directive of 1995. The LORTAD (like the GDPR) was not considered a "privacy" law because, in Spain, the right to privacy and data protection are enshrined separately as fundamental rights in our Constitution. The LORTAD regulated computerized data processing to ensure Spaniards did not see their other fundamental rights, including the right to privacy, eroded by technology. That is the core of the Spanish right to data protection as conceived by our Constitutional Court. The LORTAD did so by regulating how computerized systems handled data related to individuals, or in other words, by limiting how computers are allowed to "think" about us humans.

The LORTAD created the Spanish Data Protection Authority (AEPD), giving rise to Spain's legal data protection field. The partners at my law firm did not quite know what to do with the LORTAD, as it introduced what, at the time, were entirely new concepts into the Spanish legal system, e.g., controller, processor, and processing. That opened the door for another senior associate and me to become the leads advising clients on data protection compliance. I often tell students how we spent hours and hours for days on end trying to figure out where to provide the disclosures that the LORTAD required for transparency because what we now call "privacy notices" did not yet exist.

This field has a deep ethical dimension, which I find fascinating, so I am very fortunate to practice it after so many years.

JENNIFER: It is hard to imagine a world before privacy notices! Given your European privacy career origin, how did you transition your focus into the practice of privacy law in the U.S.?

PROF. DE LA TORRE: I moved to the U.S. in 2001 for personal reasons and could not practice law because I was only licensed to practice in Spain. The cost of attending law school in the U.S. made that option inaccessible to me. I worked as a court interpreter and taught interpretation at a local university until I learned I qualified to take the California bar exam without attending law school based on having been licensed to practice in Spain. At that point, I decided to prepare independently for the California bar exam under the supervision of Judith Saucedo, a graduate of UC Davis School of Law and an incredibly smart attorney, who chose an unconventional career path that would allow her to raise her family while making good use of her legal education by creating a business as a bar exam tutor and mentor. I passed the California bar in 2010 and became licensed in 2011. In order to forge a career path toward a practice in the area of emerging technologies in the U.S., I completed an LLM in Intellectual Property Law at Santa Clara University, and from there, I joined the eBay privacy team and, later, the PayPal privacy team.

In 2017, I was given an opportunity to return to Santa Clara University as its inaugural privacy fellow to work under Professor Eric Goldman. I welcomed it, as it enabled me to go back to teaching and to research a topic that had intrigued me for years: state privacy laws, in general, and California privacy, in particular. The timing was fortuitous as it happened before the California Consumer Privacy Act (CCPA). It allowed me to connect with Californians for Consumer Privacy and the organization behind the CCPA from almost the beginning of the process.

I did not support the 2017 initiative version because I opposed the limited access rights and the overbroad private right of action provision. However, I became a supporter when it was amended in 2018, prior to its passage through the California Assembly and Senate.

Professor Goldman placed significant trust in me by allowing me to co-direct the Santa Clara Law Privacy Certificate Program and teach Comparative Privacy at the school. In this dual role, I became aware of how experiential opportunities for law students set them on the path for career success, yet not everyone, such as first-generation college attendees, has access to them. As a consequence, today's bench of privacy practitioners is not fully representative of the population whose interest privacy laws are meant to protect. This lack of representation in our profession impedes our ability to accurately identify and remediate the biases we know can easily be inadvertently embedded in automated decision-making technologies (ADMT) and in AI.

When my fellowship ended, I joined Squire Patton Boggs, where I practiced until I was appointed to the California Privacy Protection Agency (CPPA) Board. My appointment compelled me to leave Squire Patton Boggs, as simultaneously practicing at a big law firm would have

created conflicts of interest. I took the opportunity then to create Golden Data Law (GDL).

GDL is a practice that combines my love for teaching and mentoring with my long-time passion for the practice of data protection law. GDL is a "teaching law firm" incorporated as a public benefit corporation that provides paid experiential opportunities to deserving, diverse fellows. Judith Saucedo, who taught and mentored me through my passage of the California bar exam and has since become one of my closest friends, joined GDL as the Academic Partner in 2021. The two of us have joined forces to become the engine behind the firm. For now, GDL serves the non-profit sector, as my role with the board is incompatible with advising organizations subject to CCPA. We took on clients who support our mission and were incredibly fortunate to have Candace Moore, a bright and talented Santa Clara School of Law graduate, accept a role as our inaugural fellow at the end of 2021. Candace works directly with clients under my supervision while receiving mentoring support from Judith. We expect to seek a new fellow in 2024, and grow our practice from there in order to fulfill our mission of fully preparing our fellows to enter practice in their desired sector.

JENNIFER: Thanks for sharing that interesting career trajectory, and congratulations on the founding of GDL. How do you think that your background as an EU-trained lawyer shapes your view on U.S. privacy law, and what similarities in the legal frameworks do you see?

PROF. DE LA TORRE: I have taught Comparative Privacy Law for years, focusing on GDPR and comparing it to other leading legal frameworks. That, plus my perspective as an EU data protection lawyer, has been a critical factor in shaping my views on U.S. privacy law.

I am not a proponent of importing the EU data protection framework wholesale into U.S. law. The origin of the right to data protection in the EU can be traced back to the European reaction to the rise of automated data processing in the '60s and '70s, which is closely connected to the history of the region and particularly to the use of computers by the Nazis and other authoritarian governments in Europe.

The history and culture of the U.S. is quite different. In our country, which has benefited immensely from the digital revolution, the consensus is that development and use of computerized technology should not be banned or restricted unless and until specific concerns are identified. Regulating personal data in the U.S., therefore, calls for a different approach, one that finds inspiration in the EU model while still being true to the unique American perspective. In fact, this is precisely the balance achieved by the CCPA.

The CCPA is revolutionary. It reshaped the global dialog around data and privacy for the first time since the EU enacted data protection laws in the '80s and '90s. It has spurred on other states to adopt similar laws and will certainly impact other countries. I hope that we will soon see a federal law modeled after the CCPA that does not require the pre-emption of existing, more robust state frameworks like the California one.

JENNIFER: Speaking of the CCPA, what can you share about the process for being appointed to the CPPA Board, and what drove you to seek this appointment?

PROF. DE LA TORRE: Finding an opportunity to serve in the public sector was a goal for me after my fellowship at Santa Clara Law School ended. Because of my interest in policy, the regulatory role of the CPPA, which rests in the Board and cannot be delegated, made the prospect of serving as a Board member very attractive.

That said, during the campaign for Prop 24, the initiative that amended the CCPA and created the Agency, I never expected to be considered, much less appointed, to serve as an inaugural board member at the CPPA. For one thing, I was still in the process of obtaining U.S. citizenship. Additionally, my background was primarily in the practice of law. Although I had researched and taught California privacy law, I had not written scholarly papers on the topic. I was pleasantly surprised when I was invited to share my résumé to be considered for the role. The process was similar to any other hiring process. I went through several remote interviews over a three-month period and was selected for the role. After terminating my employment with Squire Patton Boggs, and completing the rigorous disclosure process, I was sworn in and attended the inaugural meeting of the Board on July 14, 2021.

I am grateful to California's Senate Rules Committee and the President *pro tempore* of the California Senate, Senator Toni Atkins, for the trust they placed in me by appointing me to serve as an inaugural board member of the CPPA. The role placed significant responsibilities on my shoulders, but I have been able to carry it out successfully, thanks to the unwavering support of Senator Atkins's leadership staff, the collaborative and supportive culture that we created within the Board, and the colleagues and friends who have generously helped me along the way.

JENNIFER: One area that has received increased focus from California privacy practitioners is the intersection between employment law and privacy law. What do you think about the future intersection between these two disciplines in light of the CCPA's coverage of employee data?

PROF. DE LA TORRE: Applying the principles and rights enshrined in the CCPA in the context of employment law in the U.S. is new and very specific to California, as other states do not regulate employment data. However, this is not necessarily an area where guidance is missing, given that data protection compliance in employment has long been required in Europe meaning that resources are available on best practices from the local EU regulating authorities.

Beyond that, I prefer not to make any concrete statements, as the California Attorney General's office has announced an investigative sweep through inquiry letters. I understand letters have been sent to large California employers requesting information on CCPA compliance with respect to the personal information of employees and job applicants. I am confident that the California Attorney General's office will release information on the inquiry to the public when appropriate. I would encourage practitioners to pay close attention to it.

JENNIFER: Many of our CLA members serving in private practice and in-house corporate privacy positions would be curious to know how your prior roles impact your perspectives and contributions to the CPPA.

PROF. DE LA TORRE: Throughout my time at the CPPA, I have consciously worked to represent the community of responsible privacy professionals to whom I belong. Contrary to what some believe, most privacy compliance in-house professionals deeply care about privacy and work tirelessly to guide their organizations toward responsible data stewardship. In this regard, I have been influential at the CPPA in seeking transparency for the regulated community by championing the idea of an active Board that takes responsibility for policy decisions while holding the Agency accountable for executing them. During my first year on the Board, one of my areas of focus was setting up a regular calendar of meetings at which policy decisions could be made with public participation, as opposed to allowing for those decisions to be made by the Agency behind closed doors.

Moving forward, I support the creation of two permanent subcommittees for the board: one to oversee the operations of the Agency and one to direct any further changes to regulations. The first would ensure that the Agency is budgeting and expending resources responsibly and in alignment with the policies set by the Board. The second would ensure that the Board takes the responsibility for improving the regulations, which, as directed by statute, is non-delegable. This, and the appointment of staff to support the Board, will ensure it can adequately fulfill its duties in a way that would be similar to how corporate boards and other agency boards operate.

JENNIFER: You are juggling so many impressive roles at the moment. How do you do it and what is a typical day for you?

PROF. DE LA TORRE: Interestingly, both my roles as a CPPA board member and as a founding partner of GDL rely heavily on developing similar leadership skills that go far beyond technical know-how. The keys to juggling both roles are setting a strategic plan for development, understanding, and assessing the plan's financial implications, attracting talented professionals to whom tasks can be effectively delegated, and supervising their work.

My "typical" workday ranges from attending CPPA board subcommittee meetings, and reviewing legislative drafts to attending GDL dual mentorship meetings, and working with our fellow on supervising client workstreams, such as drafting EU Data Protection Impact Assessments (DPIAs). During the law school academic year, my typical workdays also include preparing and giving lectures in my role as an adjunct law professor.

As a mother of two young children, I am also juggling personal family obligations. This was especially challenging during the COVID lockdown, as it was for everyone else.

As challenging as juggling my professional responsibilities is, at the end of the day, I love what I do and the people with whom I work. I have significantly grown professionally from the experience of handling the challenges.

JENNIFER: What advice would you give law students or young lawyers trying to transition into a career in privacy?

PROF. DE LA TORRE: For California attorneys interested in the field, joining the Bar privacy section, and perhaps the IAPP or a similar industry-focused organization, would be beneficial to jump-start their careers. Learning from other established jurisdictions is also helpful. A core understanding of data protection in the EU and familiarity with the

guidelines provided by the local regulators is obviously still a must.

Privacy is booming, but it has its challenges. To become proficient at it, you need to be confident operating in grey areas and comfortable asking questions. Because regulations and guidelines can never fully stay abreast with the speed of technological development, privacy professionals have to be able to provide advice where clear regulatory guidance may not exist or is subject to interpretation.

JENNIFER: What is your prediction for the most impactful privacy issue in the next five years?

PROF. DE LA TORRE: My prediction is that the most impactful legal issue starting now and extending into the next five years and beyond is the regulation of Artificial Intelligence. From the regulatory point of view, we cannot tackle this challenge appropriately without implementing interdisciplinary approaches that include privacy law and other fields, such as I.P. law and product liability law. This is the path to human-centric A.I. technology that does not harm individuals.

We are waiting to determine if the EU will enact the proposed A.I. Regulation draft. If the Act is not enacted by the beginning of 2024, it will likely not be enacted until the end of the election cycle in Europe, which would be 2025 at the earliest. Regardless, in the U.S. it is imperative now to find answers to the most pressing questions posed by the ongoing implementation of A.I.

I am truly honored to have had the opportunity to be a core part of the team that is taking action in California. The New Rules CPPA subcommittee on which I serve recently released the draft of the new CPPA rules on risk assessments and ADMT. The proposed framework is designed to ensure the responsible use of ADMT and A.I. and to provide consumers with control over how their personal information is used. Although changes will be triggered by the feedback we expect from the Board and through the formal rulemaking process, I can confidently predict that the final rules will take a step forward toward ensuring emerging technologies, including ADMT, are designed with privacy in mind. Supporting the responsible use of ADMT, while providing appropriate safeguards, will benefit Californians and consumers across the U.S.

On a more personal note, I can predict that I will be shifting my focus to this impactful and emerging issue. Next semester, I will be teaching a law-school course entitled "AI and the Law", which is being offered for the first time at UC Davis, where many A.I. research initiatives are already thriving across campus. I am additionally involved in initiatives to seek funding that will enable UC Davis to be more actively engaged in addressing the many societal challenges that we have seen and will continue to see in this field.

ENDNOTE

* Jennifer L. Mitchell is a Partner in the Los Angeles office of BakerHostetler, where she leads the Los Angeles and Costa Mesa Digital Assets and Data Management practice. Jennifer focuses her practice on privacy compliance and advisory services. You can contact Jennifer at JLMitchell@bakerlaw.com or learn more about Jennifer's background here: https://www.bakerlaw.com/professionals/jennifer-l-mitchell/

STARTING AN INTERNATIONAL CORPORATE PRIVACY COMPLIANCE PROGRAM

Written by Lothar Determann*

When a multinational company sets out to design and implement a data privacy compliance program, they face several threshold decisions and preparatory tasks, including:

- Putting a person or team in charge of data privacy law compliance;
- Preparing a task list by identifying relevant facts, laws, and requirements;
- Defining priorities based on business objectives, enforcement risk exposure, and ease of compliance;
- Executing the task list;
- Working with internal stakeholders and outside advisors, and;
- Taking Charge.

GOVERNANCE: PUTTING A PERSON OR TEAM IN CHARGE

Someone needs to be in charge. Several individual candidates or departments in multinational companies typically control data privacy compliance, including in-house attorneys, information technology staff, human resources, and internal audit personnel. Each of these groups has different approaches, strengths, and limitations.

In-house attorneys in corporate legal departments usually take an advisory role and inform others in the organization what applicable laws require, including data privacy laws. Depending on the company culture and individual styles, the legal department may advise proactively or upon request. Lawyers interpret and apply rules, including data privacy laws, but not all attorneys are technology-savvy or good project managers.

Members of the information technology (IT) department are technology savvy but may not find it easy to understand and apply laws. IT professionals are trained in deploying and maintaining equipment, software, and services that other groups (human resources, sales, marketing, production, etc.) used to process personal data. The IT department supports these different groups and provides technology that aids other departments' business objectives. The IT department usually establishes and implements protocols to protect personal data from unauthorized access (by deploying data security measures) but rarely decides on access privileges for individuals or legal compliance matters.

Some companies have separate compliance or internal audit functions concerned with monitoring and enforcing compliance with laws and internal policies. Auditors focus on verifying that the rules or existing compliance programs are adhered to, but do not typically define the rules. You lose an extra pair of eyes if you have the same person create and audit a program and, when audit personnel conduct investigations, they are at a particularly high risk of violating data privacy laws. Investigators often want to search email boxes, computers and files, interview third parties about suspicious conduct and occasionally intercept live calls and other communications without prior notice to the data

subject. Therefore, it can be a bit like letting the fox guard the henhouse if you task audit staff with designing a privacy law compliance program.

Another option is to select individuals from data user groups within a company, such as HR or marketing. Companies that develop or sell IT products consider data privacy not only a compliance challenge, but also a business opportunity. For example, cloud computing service providers and enterprise software and data storage providers increasingly consider data privacy laws in the product development process to ensure that their customers can effectively use the products in compliance with applicable laws. Whether privacy protections are a relevant differentiator for technology providers depends much on the target audience - larger enterprise customers tend to be very focused on compliance features, whereas consumers and smaller companies may be concerned about some features (e.g., end-to-end encryption for smartphones, or online storage) but choose "free" services or convenience over data privacy considerations.

In most businesses, the person in charge of data privacy law compliance usually comes from one of the above departments or areas of specialization. Larger companies with great exposure or interest regarding privacy laws may decide to create a new department or office. Smaller companies may find it sufficient to put someone in charge on a part-time basis. If a company has a legal department, attorneys are usually involved. Often, the legal counsel takes the lead regarding data privacy law compliance. But the ideal candidate for data privacy law compliance does not necessarily have to be a lawyer, particularly if a company views data privacy more as a business opportunity than merely a legal obligation.

TOOLS AND AUTOMATION

A number of "privacy tech" and "legal tech" businesses offer software tools and other technical solutions to help companies address privacy law requirements, such as image blurring software, web cookie managers and online forms to document data protection impact assessments. Companies with mature privacy law compliance programs can benefit from automating recurring tasks, but every company must first assess its specific compliance needs, options and preferences before resorting to technical solutions. For example, a company that receives only a handful of data access requests every year, from different jurisdictions and from different groups of data subjects (e.g., employees and customers), may be better off manually processing such requests, given that initial discretion may be necessary in each case and the configuration of a tool takes up resources, too. Also, companies that have prematurely deployed tools to conduct data protection impact assessments have become suffocated by too many records that are neither legally required or practically helpful, and the superfluous records and activities sometimes conceals situations where a deeper assessment is required. While data security measures have a single goal (prevent unauthorized access to data) and are, therefore, relatively easy to automate, data privacy laws are more nuanced, requiring individual balancing decisions, and thus present much greater challenges to automate.

Even where a technical privacy protection measure offers an undoubtedly effective solution, companies need to determine first whether the technical measure is required and appropriate. For example, face blurring software is effective in protecting privacy, but a newspaper has to carefully balance press freedom and individual privacy interests to decide when blurring is appropriate. Additionally, a developer of self-driving cars must balance safety and privacy interests before opting for face-blurring measures that could render pedestrian identification less effective and hamper evasive maneuvers for safety purposes. Similarly, a company deploying a web cookie manager must first independently determine which cookies are essential to provide online services and which are truly optional and subject to user choices. Moreover, some users of tools for gap assessments, records of processing activities and impact assessments are disappointed when they realize that they still have to gather and enter all relevant information. Therefore, companies should carefully determine at the outset what specific problem a particular tool is intended to solve, whether the solution provided by the tool is legally required, the best option for the company and compare the costs and benefits associated with the tool versus manual or other approaches.

WORKING WITH INTERNAL STAKEHOLDERS AND OUTSIDE ADVISORS

SECURING INTERNAL SUPPORT

To obtain sufficient resources and support from stakeholders within a company, one must answer the "Why" question—Why is a data privacy and security program important? For some companies, compliance is a matter of risk management and avoiding sanctions and liability. Others also care about potential reputational risks and opportunities and view privacy law compliance as a differentiator. For some companies, data privacy

and security law compliance is a key precondition to selling products and services, for example, data storage or Software-as-a-Service (SaaS). When you start out implementing a compliance program in a company, it can be very helpful to prepare a brief white paper in FAQ format to raise awareness and gain support among key stakeholders within the organization.

SELECTING OUTSIDE ADVISORS

Most companies turn to outside counsel for advice about legal requirements beyond their home jurisdiction. Typically, it is too difficult and time consuming to determine the exact nature and details of formal and substantive compliance obligations in other countries, where laws may be presented in unfamiliar formats and languages.

Many companies experience one particular challenge when working with outside advisors on compliance matters: every subject matter expert (data security consultant, technology vendor or local lawyer in a particular jurisdiction) is familiar with the risks and possible sanctions in the expert's area of specialty and takes these particularly seriously, but companies tend to have a limited budget and cannot always address all requirements at once with the same rigor and effort. Companies need to prioritize. If you hire coordinated global teams, they may be able to assist with prioritization among the disciplines they are engaged to cover, but even their abilities are limited and they cannot be expected to take all fundamental considerations into account that can make or break a company, e.g., how to secure operational continuity, revenue and funding. If you hire individual advisors rather than a coordinated team, such individuals are usually not of much help with respect to prioritization and there is a significant risk that the importance of a particular risk or local law requirement is over- or understated. Therefore, it can be helpful to ask outside advisors not only about substantive and formal requirements, but also about practical issues, such as whether particular requirements are observed in practice or only honored in the breach, whether challenges by regulatory or private plaintiffs are common and what risks and problems other companies have run into in connection with the particular requirement at issue. Answers to such questions help put things into perspective and help companies prioritize among tasks.

APPOINTING A PRIVACY OFFICER

People who take charge of designing and implementing data privacy law compliance programs sometimes hold the title "Data Protection Officer" or "Chief Privacy Officer." The roles associated with these and similar titles can actually be quite different, and you should consider carefully whether your company needs one or the other or both.

GERMAN LAW ORIGINS

One key reason multinational businesses have a data protection officer is because they have a presence in Germany. Most multinational businesses consider Germany an important market. Under German data protection law, companies have been legally required to formally appoint a data protection officer with a watchdog role to supplement supervision by governmental data protection authorities since the 1970's. Germany was the first country to introduce the concept of a data protection officer in an attempt to force self-regulation via a company-appointed guardian of privacy interests.

Some jurisdictions with early data protection laws, including France, opted instead for government notification and approval requirements. There, companies have to file descriptions of their data basis and processing purposes and seek prior approval before they engage in certain activities, e.g., operating a whistleblower hotline or surveilling employees outside the scope of limited exemptions. Other countries, such as Switzerland, adopted a middle ground approach and gave companies the option to appoint a data protection officer in lieu of submitting more substantive filings to data protection authorities. According to the GDPR, companies in all EEA member states must appoint a data protection officer if they engage in particularly sensitive forms of data processing, including systematic monitoring of data subjects or processing of special categories of personal data on a large scale and as a core activity. Affiliated groups of companies can appoint one person as data protection officer for several or all entities if the person is accessible from all locations.

Some companies model their compliance approach for all jurisdictions where they appoint a local data protection officer after the German rules. This should ensure compliance with the GDPR and other countries' rules (as the German requirements tend to be the strictest and most comprehensive), but it is not legally required.

Many companies also voluntarily appoint data protection officers or privacy law compliance liaisons for countries where it is not required, incentivized, or even contemplated. In addition, many larger U.S. companies have a Chief Privacy Officer, as well as compliance officers, internal auditors,

specialized legal counsel for data privacy law compliance matters, information security officers and trained privacy professionals. The purposes, roles and responsibilities of such positions can, and often should, be quite different. If you decide to create a privacy officer position on a voluntary basis, you could define its rights and duties in reference to the data protection officer role set forth in the GDPR, and carefully decide which aspects of the statute to adopt, modify or omit.

REQUIREMENTS TO APPOINT A DATA PROTECTION OFFICER UNDER THE GDPR

According to the GDPR, companies must designate a data protection officer if they conduct regular and systematic monitoring of data subjects on a large scale or if one of their core activities is processing of particularly sensitive information, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, or health. German law is stricter and requires companies typically to appoint a data protection officer in writing within one month of commencing business. Some exceptions apply, for example, for companies that do not process sensitive data and have fewer than twenty employees.

QUALIFICATION REQUIREMENTS

Candidates must be experienced, knowledgeable or trained regarding data protection legislation, IT and the company's operations. They must also be reliable and not have conflicts of interest, which typically rules out the appointment of business owners, senior managers, and employees with a strong interest in data collection and usage, such as marketing and HR managers in the EEA (whereas officers and directors of companies can be named as responsible for data protection law compliance under Korean and Singapore law). Finally, the company must enable the data protection officer to perform the statutory obligations; this requires companies to provide information and training and to release internal data protection officers from other work duties (to free up time). Many companies appoint non-managerial employees in their legal, IT or HR departments - or contract with external service providers.

EXTERNAL VS. INTERNAL CANDIDATES

A company can appoint either an employee or an external service provider. Each option has certain advantages and disadvantages. If a German company appoints an employee as data protection officer, the employee becomes entitled to even stronger protections against termination than German labor laws generally afford all employees. Terminating an external data protection officer tends to be relatively easy by comparison, based on the terms of the applicable services contract. Appointing an employee allows the company to keep all relevant information internal and confidential. Appointing an external candidate means opening the company's systems, processes, security measures and data to someone on the outside. An internal data protection officer tends to be more familiar with actual practices, processes and problems and has better access to information about employee concerns and security weaknesses. External data protection officers may have a better feel for industry standards and more experience and expertise than internal employees who take on the position on a part-time basis. Specialization allows an external data protection officer to focus on the latest developments in data protection law and IT. Companies also consider the costs and response times: external service providers can be paid on an hourly basis (which can incentivize the data protection officer to be particularly active and responsive to inquiries and make it difficult for the company to control costs) or with a monthly or annual fixed fee (which can result in lengthy response times and thus delays in project implementation). Internal data protection officers require the company to consider the impact on the candidate's other contributions in light of the time the role as data protection officer will take.

A multinational business could appoint an employee of one of its entities outside of Germany or from another of its German subsidiaries as data protection officer if it has one. Such person could qualify as an "external" data protection officer under German law, thus avoiding the implications of German labor laws. Some German data protection authorities are skeptical about the appointment of persons who reside outside of Germany and may argue that such persons are not able to adequately perform their statutory obligations. However, German statutory law does not strictly require the appointment of an employee in Germany, and companies with headquarters and data centers outside of Germany have good reason to appoint someone outside of Germany if the person is closer to the company's regional or global systems. Multinational companies may prefer to have only one person in the role of data protection officer for any jurisdictions where the appointment is required, so that consultations on multinational projects can be conducted efficiently, quickly and without the risk of conflicting opinions and requests. In jurisdictions where the appointment must be notified to data protection authorities, companies have to be prepared to answer questions and

handle resistance to the appointment of a data protection officer who does not reside in the respective country or who does not speak the local language. In most cases it is possible to overcome the authorities' hesitations if the company has good operational reasons. The GDPR expressly allows groups of affiliated companies to appoint one single data protection officer provided that the data protection officer is easily accessible in every company and office.

APPOINTMENT FORMALITIES

Under German law, companies have to appoint data protection officers in writing. Under the GDPR, companies must publish contact details of the data protection officer and notify the data protection authority. Generally, companies prefer to assign and publish aliases (e.g., data-protectionofficer@company.com) to avoid a need to update privacy notices whenever a data protection officer is replaced. Companies may impose a time limit on the appointment, so long as the term is not so short that it interferes with the independence of the position. Two to five years seems reasonable. For German companies with a works council (collective labor representation), the works council has a co-determination right regarding changes to the employment contract for an employee is appointed as internal data protection officer.

When local law does not require or reward an appointment, companies tend not to formally appoint data protection officers. Companies that do appoint a data protection officer under the GDPR—voluntarily or not—must notify the competent data protection authorities, which could be more than 30 authorities for a U.S. company and thus very onerous.

DUTIES

The data protection officer is responsible for monitoring the company's compliance with applicable data protection law and ensuring that the company documents its data processing activities. Companies must consult with the data protection officer regarding their data processing activities and any contemplated change. The data protection officer makes recommendations and raises awareness and concerns where appropriate but does not have to formally approve measures. If the company does not act despite being formally notified of concerns, the data protection officer has the right—and in some cases the obligation—to blow the whistle and notify data protection authorities. The data protection officer operates independently and is not subject to orders or instructions from management. Day-to-day duties can include assistance with documenting data processing procedures in a register; evaluating and further developing data protection and security policies; suggesting, selecting and implementing technical security measures; drafting forms and contracts appropriate for data protection; selecting employees, service providers and others to be involved in the processing of personal data; monitoring data privacy and security measures and the proper use of data processing programs; handling complaints relating to data protection and violations of law or policies; and conducting employee training.

PERSONAL LIABILITY

In picking an employee as a candidate for data protection officer, one can expect an inquiry regarding personal liability. In short, all employees can be held liable for misconduct and violation of laws and third-party rights. Most candidates, however, are probably as much or more at risk regarding their other job duties than with respect to the role of data protection officer. German data protection legislation does not specifically address the personal liability of a data protection officer. Under generally applicable laws in most jurisdictions, any individual representative of a company can be held accountable for an act or omission of the company if the representative committed the act at issue or had a responsibility to avoid the omission. On this basis, a data protection officer can be held accountable for direct involvement in illegal data processing activities (e.g., recording of phone calls without consent or court order). Theoretically, a data protection officer could also be liable for failure to stop illegal activities that were conducted without the data protection officer's direct involvement. However, it is relatively rare that employees are charged because of a failure to act.

One data protection officer for multiple jurisdictions. Some companies appoint the same person for several or all jurisdictions where a formal appointment is required. This is expressly permitted under the GDPR and particularly efficient for companies that use global systems and procedures, which can be monitored best by one person.

INFORMAL, VOLUNTARY APPOINTMENTS

Separate and apart from satisfying formal statutory requirements to appoint a data protection officer, larger organizations often see operational advantages in

establishing a network of local liaisons for data privacy law and other compliance efforts in order to have specialized local contacts who can help implement and monitor these legal programs. Also, many companies voluntarily appoint a "global privacy officer" or "Chief Privacy Officer" to demonstrate internally and externally that the company takes data privacy law compliance seriously. It may also be beneficial to have one point person who takes ownership and responsibility for privacy law compliance—which affects many other functions, including IT, HR, physical security, legal, finance and sales.

For informal and voluntary appointments and for jurisdictions where the role of data protection officer is not defined by statute, it is important that the company define the authority and duties of the privacy officer in a detailed written memo or agreement. In particular, a company must define expectations as to whether the privacy officer will advocate primarily for privacy or company interests; provide advice or make decisions; react or be proactive. Similarly, should the privacy officer coordinate, support, supervise or monitor colleagues in roles with overlapping responsibilities (such as compliance officers, internal auditors, privacy counsel in the legal department and IT and security staff in the IT, marketing and HR departments)? Companies must decide and document the objectives and expectations: should the Chief Privacy Officer be a coordinator, advocate, advisor or guardian of privacy of the company's interests in data and compliance? Each company must make its own decisions in this respect, and each company should define responsibilities and tasks clearly in writing, so ensure the appointed individual understands the rights, obligations and expectations of the role. When roles are not clearly defined, misalignment of expectations can easily result in uncomfortable conflicts. For example, if a global privacy officer at a U.S. company understands the role as independent and public policy-driven, she might be quick to notify U.S. authorities of concerns. Or, if a member of the legal department is appointed as "Chief Privacy Officer'" and shifts from acting as legal counsel towards a more executive role, this might undermine attorney-client privilege in certain situations. Companies should consider these and other pros and cons before making voluntary appointments and document the role in detail to improve the likelihood of achieving the desired benefits and to reduce the risk of unwanted consequences and conflicts.

DESIGNATED REPRESENTATIVE

Additionally, and separately from data protection and privacy officers, the GDPR requires companies outside the EEA to designate a representative in the EEA if they process personal data of EU residents and do not maintain an establishment in the EU (such as a branch, representative office or other unincorporated presence—which most companies try to avoid for tax reasons). With this requirement, the EU wants to increase the chances for data protection authorities to reach and sanction foreign companies. The designated representative can be an individual or legal entity and has a largely passive role. The representative must be identified in privacy notices to be contacted by supervisory authorities and data subjects on all issues related to data processing and represents the non-EU-based company with respect to obligations under the GDPR. In terms of active duties, the representative shall maintain records of processing activities for the non-EU-based company, and the representative shall "cooperate" with data protection authorities on request. Multinationals should consider designating a wholly-owned subsidiary in a business-friendly EU member state where they maintain regional headquarters, servers, data processing staff and a data protection officer appointed for all their EU-based subsidiaries. By creating one center of gravity for data processing and protection activities, multinationals may be able to position one subsidiary in the EU as a group-wide "main establishment" for GDPR purposes. This could help to qualify the larger group for "one-stop-shop" treatment and sole jurisdiction of one single EU data protection authority.

Russia, Turkey and other countries have started to follow suit with similar requirements to appoint local representatives or establish presence in their territory in order to increase their chances of enforcing their laws against foreign companies. Companies with social media or other publishing businesses must carefully consider possible repercussions in their home countries if they fully submit to Russian or Turkish media laws and comply with data access and censorship orders. Also, companies should consider the impact of trade embargoes and tax implications associated with establishing presence in jurisdictions that are geo-politically at odds with their home countries.

ACTION ITEMS

1. Determine where you have to appoint a data protection officer under local law.
2. Consider internal vs. external, in-country vs. regional or global appointments.
3. Determine how your company can best achieve and maintain compliance in jurisdictions where you are not legally required to appoint a data protection

officer, and whether your company would benefit from the voluntary appointment of a Chief Privacy Officer and local liaisons; if yes, carefully document the job description, authority and duties, and consider relations to similar or overlapping functions, such as corporate legal counsel, information security, HR and marketing managers.
4. Identify and consider compliance options regarding duties to appoint local representatives.

PREPARING A DATA PRIVACY COMPLIANCE TASK LIST

Once you have put someone in charge, it is time to prepare a list of tasks and keep track of implementation status and priorities. Creating and monitoring such lists help prioritization, planning (budgets, achievements), management of complex situations (e.g., involving several jurisdictions and different types of databases) and transitioning projects from one employee to another. On a task list, you can keep tabs on formal compliance requirements (e.g., notices, filings, appointment of a privacy officer, data transfer agreements) and substantive tasks (e.g., implementing access controls, deploying encryption technologies, replacing vendors).

SAMPLE TASK LIST

For example, a U.S. company with a few foreign subsidiaries may have the following items on its initial task list - maybe supplemented by columns for status, action items and responsible persons:

1. Designate role and prepare appointment documentation for global data privacy officer; appoint local data protection officers where required, e.g., for German subsidiaries.
2. Assess where government filings (notifications, application for approvals) are required, prepare and submit.
3. Take inventory of databases and data flows.
4. Prepare and implement intra-group data transfer agreements based on EU Standard Contractual Clauses and other measures to legitimize international data transfers.
5. Review, revise and translate privacy policies and notices directed at consumers, individual representatives of corporate customers and business partners; determine how best to obtain and document consent.
6. Review or prepare notices to employees regarding processing of employee data including:
    a. Global human resources information system (HRIS)
    b. Monitoring tools and investigations
    c. Whistleblower hotline
    d. Payroll, benefits, and stock options
7. Review or prepare standard templates for data sharing or processing terms in agreements with business partners such as vendors, customers, intermediaries (resellers, sales reps for advertising services) and affiliates, including:
    a. Template data transfer contracts (intra-group and third party) and intra-group policies
    b. Data processing agreements and onboarding protocols
8. Review or develop internal protocols and processes for data access, data retention, information security, incident response and response to disclosure requests from law enforcement, regulators, or private litigants.
9. Implement global or jurisdiction-specific protocols for opt-in/opt-out processes and data security breach notifications.
10. Conduct training and audits.

PREPARATORY ANALYSIS

To define tasks for your company, you must determine what data you have, what laws apply, what the laws require and how your company can best satisfy the requirements (where the law gives you options or where resource limitations force prioritization).

Finding and analyzing all applicable laws and requirements can feel like a Sisyphean task if you work for a large organization or any business with an international scope: by the time you have taken an inventory of existing databases, usage patterns, transfer flows and applicable laws, the company has probably swapped out a few systems, acquired and spun off businesses, entered new jurisdictions and found new opportunities to commercialize data, while several new data privacy laws have been enacted. Given the rapid pace at which data privacy laws and information technology move, it is usually most effective to design and implement the data privacy law compliance program in phases. Focus first on high-risk requirements and low-

hanging fruit in both the design and implementation phase. Start with implementing high priority tasks while you are still refining the design of the program. Compile a list of known compliance requirements that your organization and your peers and competitors already try to satisfy, or that are actively enforced. When you identify compliance gaps in high-risk areas, take action immediately. After that, add tasks to the list and turn to prioritization. Companies that start by trying to develop a complete inventory of applicable legal requirements often find the challenge overwhelming and become paralyzed. In such circumstances, "perfect" can become the enemy of "good."

CHECKLIST

As you prepare your task list, you should:

1. Take inventory of your data. At the outset, consider what personal data your business uses. At a minimum, you should prepare a brief summary with basic information about your key databases, including data categories (i.e., data fields populated), primary purposes (e.g., HRIS, customer relations management (CRM), email exchange server), geographical location of servers and who has access (e.g., employees, departments and third party vendors). If you have international operations, you will also need to know names, addresses and headcount of all your legal entities and branches.
2. If you are working for a small or medium-sized company, it should not take you more than a few hours to prepare such an initial summary: you can go to the IT department, open the various software interfaces for the databases and copy basic information from screen shots; the legal department should have a list of subsidiaries and the HR department should know headcount. This is enough to get started.
3. If your company is subject to the GDPR, you have to maintain more formal and detailed records of data processing activities, including:

    a. Names and contact details of your company or companies, their representatives in the EEA and their data protection officer, if any;
    b. Purposes for the data processing;
    c. Categories of data and data subjects;
    d. Categories of recipients to whom you disclose data, including processors (and customers, if your company acts as a processor);
    e. International transfers and specific safeguards in place;
    f. Time limits for erasure; and
    g. Technical and organizational security measures.

4. If your company is subject to the CCPA, you must publish detailed lists of information that your company disclosed or sold in the preceding 12 months, applying the categories and terminology prescribed by the statute.

DATA MAPPING

Larger companies sometimes conduct more elaborate assessments and audits of databases and data flows, often with the help—and sometimes at the initiative—of outside advisors. This can be beneficial and even necessary to get a solid grip on the status of data privacy law compliance in complex multinational organizations. However, such exercises can also take a long time, use a lot of resources and produce reports with overwhelming details that do not directly translate into improvements of the organization's compliance status. Consider starting with a high level inventory unless you are fairly sure that your company is past the initial compliance phase, and you can handle a full-blown data flow mapping exercise.

DEFINING OBJECTIVES AND PRIORITIES

Companies have varying objectives regarding data and privacy law compliance. Some companies view data privacy law compliance like any other legal requirement: they want to do only what is legally required (or what is commonly done in their industry and market segment). Other companies—particularly companies with IT products or services—view data privacy as a potential competitive differentiator; consequently, they want to meet their customers' expectations, and perhaps exceed the competition.

With respect to specific aspects of data processing and compliance, objectives vary. For example, some companies depend heavily on direct marketing and may want to collect and use personal data to the maximum extent in each jurisdiction, whatever the costs may be. Whereas other companies are content to find and comply with the strictest worldwide requirement and implement a uniform compliance protocol in the interest of uniformity and cost savings. It is important to define and communicate these objectives efficiently to employees to ensure appropriate priorities are established.

FINDING THE BEST APPROACH FOR YOUR COMPANY

Based on an initial assessment of applicable requirements and company objectives, you can select an approach that suits your organization and situation:

Should you be proactive or reactive? It is usually less risky, easier and cheaper to take proactive steps to avoid a problem than to cope with a lawsuit, investigation or negative press campaign. However, only a small fraction of potential problems materialize. If cost containment is a key driver and your organization views privacy law compliance as just another legal obligation, you may consider a risk-benefit analysis and the 80-20 rule (Pareto Principle). A relatively smaller percentage of potential problems (perhaps 20% in some cases) is responsible for the vast majority of adverse impacts (perhaps 80% in some cases—but this is just an estimate). Conversely, companies can cover perhaps 80% of their problems with 20% of the budget it would take to address all problems. To address the remaining 20% of problems, which may not even be the most serious problems, the company would have to expend 80% of the total potential budget. Based on these insights, companies first try to find and rectify those problems that are most likely to result in major issues or the problems that require the least amount of effort and resources to fix.

Some problems (e.g., outdated website privacy statements) are easier and cheaper to fix than other problems (e.g., a lack of budget for encryption technology or the need to replace a legacy system that does not allow differentiated data access controls). Companies on a budget may find it easier to start with "low-hanging fruit." Most companies can quickly assess what their main competitors are doing by reviewing their website privacy statements and processing notices, determine whether particular steps are legally required and then follow suit based on precedents. This approach by no means guarantees full compliance, but it can help a company catch up to an industry standard relatively quickly and with modest resources.

If your company is or wants to become an industry leader, you must consider a more comprehensive assessment of legal requirements and business needs. You might poll stakeholders in various departments (including legal, HR, IT, sales, product management and procurement) to prepare a list of company-specific priorities, subscribe to legal and trade publications and conferences to obtain a broader picture of the compliance landscape, follow guidance from government authorities, possibly even proactively seek guidance from authorities and monitor enforcement and litigation cases.

In terms of following guidance from government authorities, it is important to determine to what extent your business is exposed to action from governments. A regulated entity (e.g., a bank or telecommunications service provider) usually has to take its regulator's views seriously whether based on law or not because it depends on the goodwill of its regulator in many respects. Entities that are neither regulated nor sell primarily to regulated entities, however, have more freedom to take independent positions and views; such entities will typically ask not only what the views of a particular government entity are, but also if and how such views are enforced. This is particularly important in gauging the relevance of official guidance from government authorities abroad. European data protection authorities, for example, have taken relatively extreme positions on various topics over many years without any enforcement activities that could have resulted in "reality checks" in court. A company that readily follows the official guidance at the expense of missing out on business opportunities may regret doing so if the guidance is not followed in practice or at some point challenged and invalidated in courts.

A company may find different approaches appropriate for a particular jurisdiction or part of its business. For example, a company with a large employee population and a hostile works council in Germany would seem well advised to be particularly proactive with respect to data privacy of German employees, whereas other jurisdictions may present less of a priority. A company with a particularly sensitive IT product (e.g., a repository of online medical records) may go out of its way to achieve or surpass compliance requirements with respect to its products, but it may decide that following industry standards suffices with respect to employee privacy. Employee privacy law compliance may be even less of a concern for a company that is still managed and operated largely by a group of founders who have a significant financial stake in the company and hence a relatively strong interest in minimizing compliance costs and efforts.

IDENTIFYING LEGAL AND OTHER REQUIREMENTS

As one identifies legal requirements for designing and updating a data privacy law compliance program, one will find thousands of laws around the world that address data privacy in one way or another. Even very large and compliance-oriented companies struggle to keep current. Smaller organizations have to establish priorities and

systems to ensure they are capable of complying with key requirements—even if they may not be able to identify each and every law in detail.

What are data privacy laws? Despite different histories and public policy motivations, there are common themes that help categorize and identify laws that are relevant to data privacy law compliance programs. Data privacy laws in the narrow sense are typically concerned with personal data (i.e., data relating to individuals as opposed to legal entities) and place conditions or restrictions on the collection, use, transfer and retention of personal data. These laws are of primary concern for those designing and maintaining data privacy law compliance programs. There are many of them, but the realm of relevant laws can be narrowed down by applying subject matter and jurisdictional filters.

Some data protection laws apply directly only to certain types of entities. For example, European data protection laws do not typically apply to data processing by national security agencies or private individuals in the course of a purely personal or household activity (e.g., what someone posts about friends on Facebook). Healthcare-related data privacy laws in the United States (e.g., HIPAA) apply only to certain "covered entities" and their "business associates," such as medical doctors, health insurers and certain service providers. Some laws relating to financial or telecommunications data apply only to banks or telecommunications providers, respectively. Anti-spam laws tend to focus on for-profit, commercial enterprises and contain exceptions for political and non-profit organizations.

If your business is—or could be—typically acting as a processor on behalf of other entities, then your compliance obligations may be much more limited and not extend far beyond following instructions from the controller and keeping data secure from unauthorized access.

Even if a certain law does not apply to your business, it may nevertheless be relevant if it applies to your business partners or clients. Most businesses, though, can remove a significant number of laws from consideration based on subject matter limitations.

INTERNATIONAL APPLICABILITY

There are more than 190 countries in the world and within each country, there may be several different jurisdictions (e.g., 50 states in the U.S.). Companies usually take a hard look at which jurisdictions they primarily must consider. Under customary international law, every sovereign country is free to legislate as it sees fit. There is no "world constitution" or treaty that limits what countries can regulate in their national laws.

Typically, countries apply their data privacy laws to organizations that are incorporated or registered in their territory or that have employees or equipment to the country. Some countries go further and apply their data privacy laws to companies abroad. For example, if a company collects data remotely via targeted websites (as indicated by country-specific URLs, languages, localized content or local phone numbers) or even just on the basis that the foreign company collects data of residents of the legislating country. Internet service providers, multinational enterprises and many other organizations with more or less direct business connections to other countries find that many countries' privacy laws apply to some of their data processing activities. However, there are also many organizations with a domestic focus which can rule out most countries' laws because they are not permitted or able to do business in other jurisdictions due to regulatory restrictions (e.g., local banks or hospitals) or resource limitations (e.g., local construction companies).

Under European Union law, member states generally may not apply their national data privacy laws extraterritorially to companies in other member states. This is intended to make it easier for companies based in the EEA to do business everywhere in the Common Market. An EEA-based controller must comply only with the national laws of the EEA member state where it maintains a branch or other significant physical presence, even if it collects data from other EEA member states (over the Internet or otherwise). This privilege is not available to companies outside the EEA. Therefore, a U.S.-based e-commerce company with customers throughout the EEA may have to comply with the laws of numerous different EEA member states. However, if it incorporates a subsidiary to become the sole contracting party and controller for all European customers, then the new subsidiary would only have to comply with the data protection laws of the jurisdiction where it is incorporated. Since the GDPR took effect in 2018, companies have become less concerned with national laws, but some differences remain, and location planning is still necessary. Companies in the United States may be able to invoke similar protections under the U.S. Constitution's "Commerce Clause" against state laws that discriminate against, or unduly burden, interstate commerce. Such jurisdictional privileges provide some companies with a planning opportunity to actively influence which laws apply to them.

If you apply the above considerations and end up with a shortlist of jurisdictions that are still too long, you can prioritize further by identifying the countries where you should be particularly concerned about enforcement. Concerns tend to be greater in countries where you have a subsidiary, employees, key assets or key customers, or where regulators are particularly active. Aside from business concerns, one should also consider where compliance is particularly easy (e.g., no language hurdles, similar legal system to your home jurisdiction). Based on such practical considerations, most companies can come up with a manageable shortlist of priority jurisdictions.

DATA PRIVACY BY REGION–AN OVERVIEW FOR ORIENTATION PURPOSES

Before you turn to an analysis of national data privacy laws, it may be helpful to take a brief look at different regional legislative approaches for orientation.

EUROPE

In Europe, data protection laws are worded very broadly and apply to most kinds of private and public sector data processing activities. Some jurisdictions (including Italy and Switzerland) even include information relating to legal entities as "personal data," but adopted the narrower definition of the GDPR after 2018. The basic premise in most European countries is that the processing of personal data is prohibited, except with valid consent from the data subject or based on another, statutory exception. For example, if a company needs to process personal data to perform a contract with the data subject, to comply with a statutory duty, to protect vital interests of the data subject, to perform a task carried out in the public interest or to pursue its legitimate interests, except where such interests are overridden by the privacy interests of the data subject. This last exception, also known as the "legitimate interest exception," requires a company to balance its own interests with those of data subjects. Before 2011, European data protection authorities had taken restrictive views on this exception, but recently acknowledged the "legitimate interest exception" as a justification of equal standing and not a matter of only "last resort," a development that may foster convergence and interoperability with U.S.-style data privacy law focused on protecting reasonable expectations of privacy. Still, consent and notice requirements are relatively stringent, international transfers of personal data outside the European Economic Area is restricted and many jurisdictions require government notification, appointment of data protection officers and other formal steps. Due to broad and undifferentiated prohibitions, companies and regulators have taken interpretative liberties in the past. Additionally, private lawsuits are relatively uncommon. These resulted in lax enforcement and uncertainties in many countries.

Europe has changed since the GDPR took effect in May 2018. This regulation constitutes the first significant update of EU data privacy laws since 1995 and it applies directly to companies and individuals (without a looking to national law). Data protection authorities are now able to levy much higher administrative fines of up to the greater of €20 million or 4% of annual worldwide revenue. Companies have stricter requirements regarding data protection impact assessments, data minimization, deletion and security breach reporting (within 72 hours). The basic default principle under the regulation remains "verboten": companies must not process personal data unless they can claim an exception from the general prohibition.

UNITED STATES

In the United States, on the other hand, the basic premise is that processing personal data is permissible. Generally, applicable privacy laws impose restrictions only when data subjects have a reasonable expectation of privacy (meaning an actual expectation that society considers reasonable). For the most part, organizations can destroy such expectations relatively easily by issuing notices informing data subjects of data processing practices. When broad, omnibus data protection laws in Europe were passed in the 1970s, legislatures in the United States decided to take a different approach and legislate only around serious problems. Consequently, legislatures passed laws to address specific types of risks and abuses. The United States now has myriad specifically scoped data privacy laws at the federal level and in the 50 states. When such laws apply, the restrictions and liabilities for violations can be surprisingly harsh, particularly for European companies entering the U.S. market expecting no significant privacy laws. For example, the California Song-Beverly Credit Card Act of 1971 prohibits retailers from collecting contact and other information from credit card holders, except as necessary to process the credit card transaction. This prohibition applies absolutely, even if cardholders consent in writing to the data collection, and it subjects merchants to significant liability and exposure to class action lawsuits. Yet the California law places no restrictions on information collected from cash-paying customers. Another example of a very strict but narrowly crafted law, the U.S. Congress

enacted the Federal Video Privacy Protection Act in 1988 in reaction to publicity around the videotape rental history of a candidate for judicial office, but the statute's prohibition against disclosing customers' video rental information does not apply to books or video games. U.S. federal law for health information privacy (HIPAA) restricts health data collection and use by "covered entities" and their "business associates," as well as providers of certain "protected health records," but not by anyone else; as a result, various online service providers are exempt from the law even though they may collect extremely sensitive health information from consumers over the Internet. Similarly, the Gramm-Leach-Bliley Act (GLB) applies only to financial service providers and not to most of the FinTech companies. In addition to U.S. federal privacy laws, organizations must assess state laws and will find that California, for example, has enacted many stringent and detailed privacy laws that close perceived gaps in federal privacy laws. Since January 1, 2020, organizations are now subject to extremely broad and extensive disclosure requirements, data subject rights and sanctions under the CCPA, which was expanded by popular ballot measure in the 2020 election and now also requires the establishment of a California Privacy Protection Agency, the first of its kind in the United States. Nevada, Virginia and other states are following California's lead and adding elements of EU-style data processing regulation to their state laws.

Consequently, organizations must carefully assess whether their contemplated activities are covered by a sector-specific federal or state law in the United States. If so, organizations may find much more rigid restrictions and exposure to liability than under European laws. However, it is possible that the contemplated activity falls outside the scope of any specific laws (based on the organization's original plan or conscious policy changes in light of the legal situation), and as a result, the organization only has to post an appropriate notice and comply with it. As in Europe, violations of U.S. law can be sanctioned by government authorities (including the Federal Trade Commission and state attorneys general). Additionally, in the United States, private lawsuits play a much greater practical role, given the possibility of class action lawsuits, punitive damages, civil jury trials and contingency fees for lawyers (who can pocket attorney's fees and a significant portion of damages awards while plaintiffs do not incur much financial risk if they engage lawyers on a contingency fee basis).

OTHER COUNTRIES

Other countries (e.g., Argentina, Brazil, Colombia, India, Israel, Japan, New Zealand, Russia and Uruguay) have modeled their laws more or less on the European templates or have pursued a hybrid approach—with some elements of the European legislation but more differentiated or lenient consent and notice requirements and less stringent administrative duties (e.g., Australia, Canada, Hong Kong, Mexico and Singapore). The People's Republic of China has traditionally focused on national security, local data storage and retention requirements, social scoring and monitoring, as well as support for technological innovation; yet, China is also working on adding EU-style data processing regulations to its national laws.

OTHER LAWS AND COMPLIANCE REQUIREMENTS

Besides data privacy laws in the narrow sense, organizations must consider a variety of other requirements when designing data privacy law compliance programs, including the following:

1. Statutory obligations under employment, consumer protection and unfair competition laws, as well as constitutional safeguards, which apply directly to companies in some jurisdictions;
2. Contractual obligations (for example, regarding data security standards, breach notifications and incorporation of privacy statements by reference in contract terms),
3. Commitments to data subjects in previous privacy policies and notices; and
4. Customer expectations and other business needs (what data do you need, for how long, for what purposes?).

Substantive compliance requirements vary significantly in jurisdictions with European-style data protection laws versus the rest of the world. However, there are also requirements that apply globally, e.g., that companies must comply with their published privacy policies.

One universal requirement is: Do what you say—comply with the limitations you state in notices, policies, website privacy statements and contracts. If a company remains silent about its data processing practices, then this requirement does not have much significance. However, in more and more jurisdictions and industries, companies are forced to issue statements and notices, either as a matter of law, industry practice or technical requirements (e.g., many mobile app stores require developers to post privacy statements). In the United States, for example,

the Federal Trade Commission urged Internet companies to publish website privacy statements early on based on unfair competition law theories, and much of the early enforcement focused on failures to comply with promises made in semi-voluntarily issued privacy statements. If companies fail to comply with their own notices, policies and statements, they can be sanctioned in most cases under various legal theories, including unfair competition laws and tort law (misrepresentation). Therefore, companies must focus on keeping their notices, privacy statements, contracts and other privacy-related communications accurate and up to date–either by adapting their communications or their practices.

DATA SECURITY

Organizations must maintain reasonable security measures to keep confidential data protected against unauthorized access and dissemination. Security requirements also follow from trade secret laws and confidentiality agreements and extend beyond personal data. The reach of trade secret laws ends once the secret is disseminated. Data protection laws also require reasonable security measures and can apply even to personal data that has become public. Therefore, the typical definitional carve-outs in confidentiality clauses (independently developed information, information in the public domain, or compelled disclosures) may not be used in the data protection law context. Organizations must comply with data protection law requirements separately and in addition to compliance with trade secret laws and contractual confidentiality obligations.

Organizations around the world have been obligated for decades to keep personal data secure under statutes and contracts. In the past, most laws and contract clauses simply set forth a general reasonableness standard and did not prescribe specific safeguards. More recently, after California enacted the world's first data security breach notification law in 2002 and organizations started reporting security breaches en masse, more and more jurisdictions have passed data security breach notification laws, and lawmakers around the world have started prescribing very specific technical and organizational measures intended to ensure that companies take more comprehensive steps to prevent security breaches and protect the data and privacy of consumers, employees and other individuals.

The extent to which companies collect, store, manipulate, transfer and otherwise process personal data depends on their business needs and legal obligations in collecting and retaining information. All businesses process some personal data. At a minimum, they process the contact information of their own employees, customers and business partners. Most businesses also process more sensitive data, such as payroll information, consumer purchase histories, data from credit card transactions and other financial and medical data. So, as part of implementing a data privacy law compliance program, one must assess the specific requirements of one's business regarding data security and develop an information security program that is appropriate for one's organization, considering specific legal requirements of the jurisdiction, one's risk profile and tolerance, as well as contractual and practical necessities.

Successful data security programs typically involve the following parameters:

1. Methods for keeping track of where data is stored and secured and for what purposes and how long it is needed;
2. Physical and technical protection for premises, networks and devices (including encryption, firewalls, strong authentication and passwords);
3. Access controls within the organization ("need to know"-based restrictions),
4. Employee training;
5. Secure deletion of data that is no longer needed (e.g., on discarded devices, paper),
6. Ongoing monitoring plus random audits and investigations into data security, performed by internal resources or external validation providers;
7. Prudent vendor selection, management, monitoring and contracting;
8. Proactive privacy impact and security-by-design assessments before any major changes to data processing activities, including the implementation of new products, processes and data uses; and
9. Security incident preparedness, based on protocols for how to report and respond to incidents, training, remediation processes, and "dry run" exercises.

As a first step, one should determine whether an organization has written policies or unwritten processes addressing these points and identify the persons in charge of ensuring compliance. As a second step, one might prepare a written summary of existing measures and then assess whether these measures meet legal requirements (legal and contractual) and adequately address risks threatening the organization. Next, one might consider validating the security program by outside advisors to confirm alignment with industry practice. It is important to reach a clear understanding and agreement

with the outside advisor on objectives and deliverables. Some organizations experience frustration because they hire data security consultants who deploy an infinite number of scans and tests but are not willing to advise when enough is enough or to issue an opinion regarding the adequacy of the organization's security efforts.

REGIONAL, SUBSTANTIVE DATA PRIVACY LAW COMPLIANCE REQUIREMENTS

Under European data protection laws organizations must satisfy a number of additional substantive data protection law compliance requirements:

1. minimizing data processing and limiting retention times;
2. maintaining data integrity by updating, correcting or deleting data;
3. granting access to data subjects on request; and
4. seeking consent or other justifications.

These requirements apply in most European countries but may not apply outside of Europe. Many countries have consciously opted against data minimization requirements because they constitute a particularly severe restraint on innovation, economic liberties and freedom of information.

FORMAL COMPLIANCE REQUIREMENTS

Several data privacy law compliance requirements are "formal" in the sense that they require generating certain notices, government filings or other paperwork. Such formal compliance obligations do not directly require changing one's data processing activities. However, if you are not substantively in compliance you are usually unable to issue appropriate notices or government filings, because you would just be notifying everyone that you are not in compliance. Substantive compliance logically comes first. Practically, it is often most efficient to start work on formal compliance tasks because this work will help identify substantive compliance requirements and gaps. Additionally, most companies find it comparatively easy to achieve formal compliance and see a particularly high risk associated with failing to comply with formal requirements, as such failures are especially easy for government investigators, private plaintiffs and other potential adversaries to prove. The question "Did you make the required filing or not?" tends to be more black and white than, for example, "Is a three year data retention time period appropriate for employee records after termination?"

As a general matter, one can expect formal requirements to typically include the following:

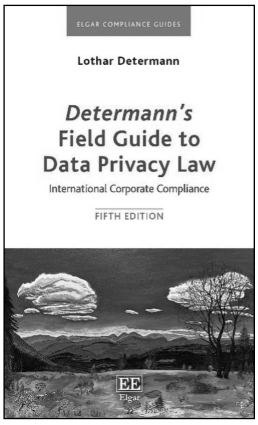
1. appointing a data protection officer;
2. preparing records of data processing activities;
3. documenting data security measures;
4. concluding appropriate data transfer or processing agreements with affiliates, service providers and other business partners;
5. issuing notices to data subjects, obtaining consent;
6. submitting notifications to data protection authorities or seeking their approvals; and
7. consulting with works councils, labor unions or other employee representative bodies, if any.

CONCLUSION AND EXECUTING TASKS

Once you have prepared a list of concrete tasks to achieve compliance with data protection laws, you should start executing those tasks, perhaps first on low-hanging fruit and tasks that help mitigate major risks. Many companies find it helpful to start preparing the required notices to data subjects because in the process they naturally go over the status quo and can then best address gaps and other issues. An important practical point is: don't get overwhelmed. It is better to close some compliance gaps than none; and even though many tasks are interconnected, it is often possible to complete tasks in some areas without prejudice to others (e.g., address employee data privacy and security before or after tackling consumer data privacy, and approach compliance for some priority jurisdictions before turning to others).

ENDNOTE

* LOTHAR DETERMANN is a Partner at Baker McKenzie, Palo Alto, California. Lothar's practice is focused on data privacy law compliance, information technology, copyrights, product regulations, and international commercial law. He is the author of California Privacy Law - Practical Guide and Commentary, 4th Edition (2020) and *Determann's Field Guide to Data Privacy Law*, 5th Edition (2022), which is also available in Chinese, German, Hungarian, Italian, Japanese, Portuguese, Russian, Spanish and Turkish.



CALIFORNIA PRIVACY LAW AND THE IMPACT ON AD TECH

Written by Daniel Goldberg and Bram Schumer*

California continues to lead the nation with new laws, regulations, enforcement actions, and court decisions relating to privacy compliance. These efforts have profoundly impacted the companies involved in the ad tech ecosystem. This article provides a high-level overview of the ad tech ecosystem, outlines some of the major California privacy developments in 2023 impacting the ad tech ecosystem, and concludes with practical steps companies in the ad tech ecosystem can take to reduce risk.

WHAT IS AD TECH?

Ad tech (short for advertising technology) refers to those technologies used to buy, sell, and manage digital advertising. The ad tech ecosystem comprises advertisers (companies that buy ads), publishers (companies that sell ad inventory), agencies (companies that help manage buying and selling for advertisers and publishers), ad networks (companies that sell ad inventory from many publishers), technology providers (companies that offers the tools to facilitate this process), and other related parties. Most companies have some relationship with the ad tech ecosystem, often in connection with their monetization models. According to a study[1] by Allied Market Research that was reported in Forbes[2], the ad tech ecosystem was valued at $748.2 billion in 2021, and could reach $2.9 trillion by 2031.

Ad tech relies heavily on the use of data. For example, to deliver an ad, a publisher must collect some data about the device where the ad is delivered. This data is collected through invisible tracking technologies, such as cookies and pixels, embedded within the publisher's website. In addition to delivering ads, these tracking technologies, often licensed from third party providers, can collect data for purposes such as research and analysis, attribution and measurement, and targeted advertising shown to the device. Advertisers can also place tracking technologies on their own websites and within their ads. In the app environment, most companies use SDKs (short for Software Development Kit) instead of cookies and pixels, to provide various functionalities offered by the third-party providers. Some of the most well-known third-party providers include Meta and Google.

Another aspect of ad tech involves data matching. To improve campaign performance and deliver targeted advertising, an advertiser or publisher may upload its first party data to a technology provider (sometimes called a clean room) to match against third party data. The uploaded data may be in the form of an email address or device identifier that is hashed prior to sending.

Takeaway. As a result of its heavy reliance on data, the ad tech ecosystem has become associated with privacy concerns. Over the past decade, California lawmakers and regulators have taken the position that most of the data processed through the ad tech ecosystem, even when hashed, is personal information subject to privacy law, and taken measures to regulate such processing.

CALIFORNIA PRIVACY DEVELOPMENTS

Below are some of the major California developments in 2023 impacting the ad tech ecosystem:

- **Do Not Sell or Share Rights under CPRA**

  In January 2023, the California Privacy Rights Act ("CPRA") took effect. One major aspect of the CPRA is that consumers have the right to opt-out of the "sale" or "sharing" of their personal information. Under CPRA, a "sale" is broadly defined to include a disclosure of personal information to a third party for something of value, and a "share" is broadly defined to include a disclosure of personal information to a third party for cross-context behavioral advertising (i.e., targeted advertising). CPRA also requires companies to process opt-out preference signals, such as Global Privacy Control[3] ("GPC").

  Takeaway: Ad tech inherently involves activities that constitute sales or shares under CPRA. Companies that use tracking technologies or engage in data matching activities could be found to be selling or sharing personal information, and need to comply with the obligations relating to sales and shares.

- **Contractual Obligations under CPRA**

  As part of the CPRA, California was required to issue implementing regulations. In March 2023, California finalized its CPRA regulations[4] and filed them with the Secretary of State. The CPRA regs add robust obligations around sales and shares, including specific language required in contracts with third parties. The CPRA regs also specify that a service provider cannot contract to provide targeted advertising services. This effectively means that companies in that ad tech ecosystem may not be able to position themselves as service providers, and instead should include specific language in their contracts regarding their obligations as third parties.

  Takeaway: Notably, the CPRA regs were set to take effect in July 2023, but the Sacramento County Superior Court issued a decision[5] delaying their enforcement until March 2024. March 2024 is quickly approaching, and companies in the ad tech ecosystem should be ready for compliance well before then.

- **Sensitive Data Rights under CPRA**

  Another aspect of the CPRA is that consumers have rights around their sensitive personal information. Under CPRA, sensitive personal information includes precise geolocation, racial or ethnic origin, religious or philosophical beliefs, health data, sex life, and more. Companies collecting sensitive personal information may only use that information for permissible purposes (such as preventing security incidents, resisting fraudulent activities, ensuring the physical safety of others, and maintaining product safety or quality). Where a company uses sensitive personal information for non-permissible purposes, it must provide consumers with a right to limit the use or disclosure of their sensitive personal information to the permissible purposes. The CPRA regs specify further obligations around implementation of this right.

  Takeaway: Ad tech often involves the collection of sensitive personal information. For example, a ride share app may request precise geolocation for the purpose of locating a ride. If the ride share app includes an advertising SDK embedded within the app, that SDK may also receive the precise geolocation, and use that data for advertising purposes (which would be considered a secondary purpose). Under CPRA, if a consumer limits the use or disclosure of their sensitive personal information, the app developer likely would be prohibited from sharing the precise geolocation with the advertising SDK.

- **Reasonable Expectation Test under CPRA**

  Although the CPRA establishes an opt-out regime, it also specifies that companies must obtain opt-in consent for any data practices that are not consistent with a consumer's "reasonable expectation." What constitutes consumer reasonable expectation is a question of fact. Under the CPRA regs, to determine reasonable expectation, a company must evaluate the relationship between consumers and the company, the type, nature, and amount of personal information collected, the source of the personal information and the method for collecting it, the specificity of disclosures made by the company about the practice, and the degree to which third party involvement is disclosed to consumers.

  Takeaway: This factor test could establish a *de facto* opt-in regime for certain parts of the ad tech

ecosystem. For example, in the rideshare example above, California regulators could determine that collecting precise geolocation data for advertising purposes always fails the reasonable expectation test, and thus requires opt-in consent—a position consistent with many other frameworks found in US privacy law, including from the FTC.

- **Protecting Children under California Privacy Law**

  Protecting children's personal information in the context of targeted advertising has become a top priority for lawmakers and regulators at every level, and California is no exception. The main US privacy law that regulates children's personal information is the Children's Online Privacy Protection Act ("COPPA"). Now over two decades old, COPPA requires websites and online services to obtain verifiable parental consent before collecting personal information (including device identifiers) from children under 13 unless an exception applies. CPRA added obligations that companies obtain opt-in consent for sales or shares of personal information of consumers aged 13 to 15. California regulators can bring an action under state consumer protection laws for alleged violations of COPPA and CPRA, and there have been indications that California regulators have issued warning letters and met privately with companies in the ad tech ecosystem relating to their use of children's personal information.

  California also has been working toward interpreting obligations under its Age-Appropriate Design Code law ("AADC"), which lawmakers passed in September 2022. The California AADC, modeled after the United Kingdom's AADC, aims to protect the privacy and data of children under 18 when they use online services, products, or features that may affect their mental, physical, and emotional health. Notably, targeted advertising is considered inherently detrimental to the health or wellbeing of children, and is arguably entirely prohibited (even with parental consent) under the law. The California AADC was set to take effect July 2024, but was recently stayed[6] by a California court on first amendment grounds.

  Takeaway: Ad tech often involves the collection of personal information from children and minors, implicating these laws.

- **New Data Broker Obligations**

  In October 2023, California passed the California "Delete Act," which introduces new requirements for "data brokers". Under the law, a data broker is defined as a company "that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Like the national "Do Not Call" registry, the Delete Act will create a centralized mechanism where consumers can submit a single delete request that *all* registered data brokers in California must honor. If a registered data broker denies a deletion request subject to an exception, the data broker must treat the request as an opt-out of sales or shares. This one-step registry must be created by the California Privacy Protection Agency ("CPPA") by January 2026, and honored by data brokers starting August 2026.

  Takeaway: Many companies in the ad tech ecosystem qualify as data brokers and will need to comply with these obligations.

- **Litigation Over Tracking Technologies**

  In the past year, there has been a significant increase in class action litigation relating to tracking technologies based on alleged violations of the California Invasion of Privacy Act ("CIPA") and federal wiretapping and video privacy laws. Plaintiffs claim that companies shared their personal information with third parties through tracking technologies without their consent, thereby violating CIPA. Many of these actions involve "session replay" technologies, chatbot technologies, and the popular Meta and Facebook pixels.

  Takeaway: Tracking technology litigation has exploded in the past year, in part due to a decision by the 9th Circuit Court of Appeals reversing[7] the District Court's dismissal of a tracking technology case.[8] As a result, many companies have chosen to settle these claims out of court rather than risk a potential adverse ruling. Of the pending actions, many are still in the motion to dismiss phase, or with plaintiffs given leave to amend their complaints. Given that the plaintiff's bar interpretation of opt-in consent under CIPA seemingly contradicts the opt-out framework under the CPRA, this area of litigation may be short-lived.

STEPS COMPANIES CAN TAKE

As California's statutory, regulatory, and litigation landscape continues to develop, companies–particularly advertisers, publishers, and other entities within the ad tech ecosystem–should consider the following steps to reduce risk and demonstrate good faith efforts in the eyes of regulators:

- **Address Do Not Sell or Share Obligations under CPRA**

  All companies–in and out of the ad tech space–should review and revise their privacy policies to accurately and comprehensively communicate their practices regarding their collection and handling of personal information, how it is used, and how consumers can exercise their rights. Among these rights, the right to opt out of sales and shares is of particular concern for regulators.

  Companies that use advertising tracking technologies within their websites or apps should consider themselves sellers/sharers of personal information, and place a link in the footer of their websites that reads either "Do not sell or share my personal information" or "Your Privacy Choices".[9] This link should allow consumers to turn off or limit disclosure of their personal information collected through advertising tracking technologies. In addition, if a company builds any internal lists–or "audiences"–of its consumers, such as for data matching purposes, the link should also direct consumers to a short form where they can enter their contact information to be excluded from audience lists moving forward. Companies must also configure their websites to listen for and process GPC signals.

  In many cases, companies will need to engage a privacy vendor to assess the use of tracking technologies, categorize those technologies to determine which ones are used for marketing and advertising, and develop backend functionality to effect consumers' opt out requests and honor GPC signals.

- **Address Obligations for Sensitive Personal Information**

  Companies should always understand what sensitive personal information they collect and how it is used. Companies that process information from or concerning children, consumer health, precise geolocation, or other high risk data sets should be particularly diligent in their analysis.

  As a best practice, companies should collect sensitive personal information only when necessary, and when they understand the purpose(s) for its collection. Privacy policies must disclose all sensitive categories of personal information that are collected, and the corresponding purpose(s). If a company uses sensitive personal information for any secondary purpose(s) (i.e., purposes that are not "permissible" under the CPRA), it must provide consumers with a notice of their "right to limit" the use of their sensitive personal information, and explain how to make that choice. To do this, as noted above, companies must place a link in the website footer that reads "Limit the use of my sensitive personal information" or use the "Your Privacy Choices" link. The latter is an omnibus solution for consumers to exercise both their right to opt out of sales/shares, and their right to limit. The link should direct consumers to a mechanism where consumers can exercise their right.

  Privacy vendors and counsel can help audit and categorize uses of sensitive personal information and develop mechanisms to comply with the right to limit.

- **Conduct Due Diligence for Vendors**

  Companies should conduct due diligence around their use of vendors, including tracking technology and clean room providers. Due diligence includes ensuring vendor contracts contain appropriate terms and restrictions around data use, reviewing code and platform functions and configurations for vendor technology, and considering vendor reputation. To the extent possible, companies should also understand data flows through vendor technology.

  In some instances, use of specific types of technology may pose unreasonable risk to a company. For example, as noted above, the use of session replay technology and interactive website chatbots has led to significant litigation in the past year. Companies may consider discontinuing

their use of these technologies until the litigation landscape in California becomes more clear.

- **Evaluate Data Broker Requirements**

  Many companies in the ad tech space can be classified as data brokers under existing California law, and are already subject to a number of obligations. The Delete Act builds upon these obligations. In order to comply today, and prepare for the Delete Act, companies should evaluate their obligations under data broker law, including the registration and annual fee requirements.

  While data brokers–like all companies subject to CPRA–already are required to honor a consumer's right to delete personal information, data brokers should start considering how they will address new obligations under the Delete Act, including deletion requests via the state's forthcoming centralized deletion portal as well as new reporting requirements. The practical impact of the deletion portal may be that data brokers treat requests as opt-outs, effectively creating a centralized opt-out mechanism.

- **Conduct Data Protection Impact Assessments (DPIAs)**

  In ad tech, conducting DPIAs has emerged as a crucial step toward responsible data handling. DPIAs serve as a systematic evaluation of the potential risks and impacts associated with the processing of personal information, especially when the data is sensitive. By undertaking these assessments, companies can identify and mitigate risks before they escalate, ensuring that both their operations and data practices align with regulatory expectations, new statutes such as the AADC, and best practices. Moreover, regularly conducting DPIAs signals to stakeholders and consumers that the company is proactive and committed to safeguarding personal information. DPIAs can also help address the reasonable expectation test under CPRA.

  Companies should complete DPIAs for every new processing operation involving personal information that presents a potential heightened risk to the consumer, which includes targeted advertising. As the requirements and processing activities that merit DPIAs takes shape, companies should engage counsel to assist with their drafting.

- **Develop a Data Governance Framework**

  A "data governance framework" is a structured approach to managing and ensuring the accuracy, consistency, usability, security, and availability of a company's data assets. It consists of policies and procedures developed by the company, and should take into account all the suggestions in this article, and more. With the evolving landscape of privacy laws and increased regulatory scrutiny, implementing a framework has become imperative to demonstrate compliance with the law and to help stakeholders understand and address their obligations within the company.

ENDNOTES

* Daniel M. Goldberg is Chair of the Privacy & Data Security Group and Chair of the Advertising Technology Group at Frankfurt Kurnit. Based in California, he is consistently recognized as one of the nation's leading data lawyers and voices on California privacy law. He routinely advises on matters involving advertising technology and artificial intelligence (AI), and is known for his ability to translate complex technical and legal concepts into actionable items. Please see his full bio at https://fkks.com/attorneys/daniel-goldberg.

Bram Schumer is an associate in the Privacy & Data Security Group at Frankfurt Kurnit. He helps clients comply with the array of federal and state privacy laws and platform obligations, including relating to use of advertising technology. He negotiates complex data-driven deals, such as those involving clean rooms and media buys. Please see his full bio at https://fkks.com/attorneys/bram-schumer.

1. https://www.alliedmarketresearch.com/adtech-market-A53696
2. https://www.forbes.com/sites/forbestechcouncil/2023/08/29/adtech-market-is-booming-how-to-benefit-from-this-growth/?sh=54157f4b3bd4
3. https://globalprivacycontrol.org/
4. https://cppa.ca.gov/regulations/pdf/20230329_final_regs_text.pdf
5. https://content.mlex.com/Attachments/2023-06-29_4745C8U6094V3K3O%2FCU_34-2023-80004106-CU-WM-GDS_10a66e19-7726-4167-bfca-5c1591881c5f8.pdf

6. https://netchoice.org/wp-content/uploads/2023/09/NETCHOICE-v-BONTA-PRELIMINARY-INJUNCTION-GRANTED.pdf

7. https://cdn.ca9.uscourts.gov/datastore/memoranda/2022/05/31/21-16351.pdf

8. Ultimately, the District Court dismissed Javier's case with prejudice, after many rounds of motions and amended complaints. *Javier v. Assurance IQ, LLC*, No. 20-CV-02860-CRB, 2023 WL 3933070 (N.D. Cal. June 9, 2023).

9. The blue symbol is required under the CPRA regs to appear next to the "Your Privacy Choices" link in the website footer.

WHAT FUTURE FOR CROSS-BORDER TRANSFERS OF PERSONAL DATA?

Written by Paul Lanois

In today's globalized world, cross-border data transfers have become a routine aspect of virtually every business operation. However, organizations that do business internationally are likely to be subject to the General Data Protection Regulation (GDPR). As a result, the organizations must comply with certain requirements, which are laid out in Chapter V of the GDPR. Since the Court of Justice of the European Union (CJEU) issued what is now known as the *'Schrems II'* decision in July 2020[1] invalidating the EU-US Privacy Shield Framework (which was used by thousands of organizations to transfer data from the EU to the US), many organizations are struggling to figure out how they can continue to transfer personal data outside the EU while still complying with the GDPR's requirements.

Following the *'Schrems II'* decision, many organizations have relied on the EU Standard Contractual Clauses (SCCs)[2] to perform their data transfers–but the SCCs are not "magic bullets" and do not automatically make a data transfer legal.

Notably, in May 22, 2023, the Irish Data Protection Commission (DPC) held that Meta Platforms Ireland Limited infringed GDPR Article 46(1) (the rules requiring appropriate safeguards for international data transfers in absence of an adequacy decision) by continuing to transfer personal data to the US following the *'Schrems II'* decision. This is even though Meta used the latest 2021 EU SCCs for the transfers and had put in place additional supplementary measures. Specifically, the DPC "*found that these arrangements did not address the risks to the fundamental rights and freedoms of data subjects that were identified by the CJEU in its judgment.*"[3]

This article will provide an overview of GDPR's regulations for cross-border data transfers and discuss best practices for managing these transfers while ensuring compliance with the GDPR's requirements.

WAIT . . . WHAT EXACTLY IS A 'DATA TRANSFER'?

The GDPR applies to any "*transfer of personal data to a third country or to an international organization.*" However, such term is not defined in the GDPR. Regulatory guidance from the European Data Protection Board (EDPB)[4] indicates that there is a 'transfer' within the scope of Chapter V of the GDPR if each of the following three criteria are met:

1. The data exporter (whether a controller or a processor) is subject to the GDPR for the given processing;
2. The data exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller, or processor; and
3. The data importer is in a country outside the European Economic Area, irrespective of whether such data importer is itself subject to the GDPR for the given processing.

The EDPB's above second criteria specifies that a transfer must involve the transmission of data from one controller or processor to another controller or processor. Importantly, the EDPB's guidelines specifically indicate that this "*second criterion cannot be considered as fulfilled where the data are*

disclosed directly and on his/her own initiative by the data subject to the recipient."[5] The term "on their own initiative" seems to cover situations where individuals, of their own accord, complete online forms or make a purchase from an online store established outside the EU.

There was previously a lot of confusion on this point, as some commentators had assumed that the collection of personal data directly from individuals located in the EU required the organization to have in place a valid transfer mechanism. Since SCCs could not be signed with individuals, those organizations turned to their EU offices to transfer the data, relying on the SCCs to do so.

DOES CHAPTER V OF THE GDPR COVER INTRA-GROUP TRANSFERS?

In case there was still any doubt, intra-group transfers of data must also be considered: the EDPB confirmed that "*data disclosures between entities belonging to the same corporate group (intra-group data disclosures) may constitute transfers of personal data*."[6]

What constitutes a 'transfer' is particularly broad, since according to the European Data Protection Board, *"examples of how personal data could be "made available" are by creating an account, granting access rights to an existing account, "confirming"/"accepting" an effective request for remote access, embedding a hard drive or submitting a password to a file. It should be kept in mind that remote access from a third country (even if it takes place only by means of displaying personal data on a screen, for example in support situations, troubleshooting or for administration purposes) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer,"*[7] provided of course that the three criteria outlined above are met.

However, not all transfers are necessarily in scope: employees who travel on business to a country outside the EU and who bring with them their laptops to work remotely would not be deemed transferring data, since employees are not separate controllers, but rather integral parts of their organization.

WHEN PERSONAL DATA CAN BE TRANSFERRED UNDER THE GDPR?

Article 44 GDPR prohibits transfers of personal data outside the European Economic Area (EEA) unless the transfer fits within one of the narrow exceptions laid out under Chapter V of the GDPR. On this basis, the first question to ask before personal data subject to the GDPR can be transferred outside the EEA is whether the European Commission has reached an "adequacy decision" about the country where the data recipient is based (Article 45 GDPR). If there are any onward transfers of personal data from one country to another country, any such subsequent transfer of data also needs to be reviewed.

As stated by the EDPB, "in the absence of such adequate level of protection" provided by an adequacy decision, the second step is to review the "*implementation by the exporter (controller or processor) of appropriate safeguards as provided for in Article 46*."[8]

The main types of transfer instruments listed in Article 46 are:

- Standard Contractual Clauses (SCCs);
- Binding Corporate Rules (BCRs) in accordance with Article 47 GDPR;
- Codes of conduct;[9]
- Certification mechanisms;[10]
- Ad hoc contractual clauses;
- International agreements/ Administrative arrangements.[11]

ARE WE SAFE TO JUST RELY ON THE NEW SCCS?

On May 22, 2023, the Irish DPC issued[12] an administrative fine in the amount of 1.2 billion euros against Meta Platforms Ireland Limited after examining the basis on which the company transfers personal data from the EU/EEA to the US in connection with the delivery of its Facebook service.

Like many businesses, the company relied upon the standard contractual clauses (SCCs) issued by the European Commission on June 4, 2021[13] following the *'Schrems II'* decision. The DPC nevertheless held that the company was in breach of Article 46 (1) GDPR as it is subject to U.S. surveillance laws, including the U.S. Foreign Intelligence Surveillance Act (FISA) Section 702. According to the DPC, such surveillance laws allow the U.S. government to access personal data of EU citizens even where additional safeguards are in place and, as a result, "*the 2021 SCCs cannot compensate for the inadequacies in the level of protection afforded by US law*."

While the DPC's ruling (and the fine imposed) is significant, the DPC decision does not necessarily spell doom and gloom for all organizations. The *'Schrems II'* decision requires each exporter to assess the laws of the destination country to ensure that the use of SCCs properly protects the data transferred in that context. The DPC's decision does not change this. Importantly, the DPC decision does not appear to exclude a "risk-based approach" that would consider the likelihood of government access pursuant to FISA Section 702. The issue in the case of Meta Ireland was that the company had received a number of government requests. An argument could be made that companies which do not receive a significant number of government requests may continue to apply a risk-based approach.

Finally, the decision notes that encryption measures implemented in respect to data in transit *may* provide appropriate safeguards in the context of Section 702. However, the DPC found that Meta Ireland had not implemented technical measures which would provide appropriate safeguards to data subjects from government requests for data through compelled assistance.

WHAT IS THE CURRENT US FRAMEWORK?

On October 7, 2022, President Biden signed Executive Order 14086 "Enhancing Safeguards for United States Signals Intelligence Activities" (EO 14086).[14] EO 14086 introduces new safeguards in relation to U.S. signals intelligence activities. According to the European Commission, the framework created by EO 14086 "*address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020*" [15] limiting access to EU data by US intelligence services and establishing a Data Protection Review Court.

Importantly, not only do they form the basis of the adequacy decision by the European Commission[16] for transfers made under EU-U.S. Data Privacy Framework (DPF), but they also provide greater legal certainty for companies transferring personal data from the EU to the U.S. using *other* transfer mechanisms, such as the Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). As stated by the European Commission, "*all the safeguards that the Commission has agreed with the US Government in the area of national security (including the redress mechanism) will be available for all transfers to the US under the GDPR, regardless of the transfer tool used.*"[17]

EO 14086 introduces new safeguards with respect to the collection of personal data by U.S. intelligence agencies:

- First, it places new requirements on the collection and handling of personal data by U.S. intelligence agencies. According to EO 14086, these protections apply to "*all persons, regardless of their nationality or wherever they might reside.*" It further requires that signals intelligence activities must be "necessary" and "proportionate" to advance a validated intelligence priority and that such activities must be undertaken in pursuit of one of the twelve enumerated national security and intelligence objectives listed in EO 14086. By way of example, such objectives include 'protecting against transnational criminal threats', 'protecting against espionage, sabotage, assassination, or other intelligence activities', 'protecting against terrorism', 'understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry', as well as 'understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation'.
- Second, it expands the oversight of signals intelligence programs by U.S. government agencies. The Civil Liberties Protection Officer (CLPO), appointed by the Director of National Intelligence (DNI), must conduct an assessment prior to any new intelligence-gathering operations. According to EO 14086, the assessment should consider "all relevant factors" and "the privacy and civil liberties of all persons" and determine if the collection activity "is necessary to advance a validated intelligence priority". Bulk collection may only be authorized where the intelligence cannot be reasonably obtained through targeted collection. Additionally, intelligence agencies must maintain documentation regarding their collection of personal data through signals intelligence and update their policies and procedures to ensure effective oversight of the new safeguards.
- Third, it creates a redress mechanism for individuals from "qualifying states" who claim their personal data has been collected unlawfully through signals intelligence programs. On June 30, 2023, Attorney General Merrick B. Garland designated the European Union along with the three additional countries making up the European

Economic Area (EEA) as "qualifying states" for purposes of implementing the redress mechanism established in EO 14086. The United Kingdom was subsequently designated as a "qualifying state" on September 18, 2023. Accordingly, individuals can now lodge a complaint with the CLPO, which has the power to investigate complaints and render binding decisions against intelligence agencies. Individuals can also appeal decisions by the CLPO before the Data Protection Review Court (DPRC), which has been established through regulations issued by the U.S. Attorney General. On November 14, 2023, the Office of Privacy and Civil Liberties announced the first panel of judges appointed to the Data Protection Review Court (DPRC). The DPRC will independently review determinations made by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI) in response to qualifying complaints sent by individuals through appropriate public authorities that allege certain violations of U.S. law in the conduct of U.S. signals intelligence activities. The Attorney General may not interfere with a review by a DPRC panel of a determination the CLPO made regarding a qualifying complaint, and the judges may not be removed or otherwise subjected to adverse action arising from their service. Individuals will be represented before the DPRC by special advocates and the decisions of the DPRC will be final and binding.

According to the European Commission, these new safeguards "*are significant improvements compared to the Privacy Shield*" and "*address the concerns raised by the Court of Justice of the EU in the Schrems II judgment and provide a durable and reliable legal basis for transatlantic data flows.*"[18]

The sharp-eyed reader may notice that EO 14086 predates the DPC's decision mentioned above and may therefore wonder what this means for the scope of EO 14086. The DPC noted that the "*DPC is under an obligation to give effect to the law as it currently stands*" and that EO 14086 is "*not, in fact, operational. More particularly, and as explained above, in the absence of designation of the EU as a "qualifying state", the new scheme is not operational at all for EU citizens.*" Given the fact that the various components of EO 14086 were not fully in place at the time of the decision, EO 14086 could not be relied upon yet. Those missing components are now operational, so a data protection authority may take a different approach if it were to examine similar facts today. Having said that, and as noted by the DPC, "*the privacy and civil liberties safeguards introduced by EO 14086 do not appear to be intended to apply retrospectively,*" meaning that transfers which took place prior to EO 14086 being fully effective would likely not be able to enjoy from its safeguards.

ENDNOTES

* Paul Lanois is a Director at the European law firm Fieldfisher based in the Silicon Valley, California, where he advises clients on information technology as well as compliance with data protection, privacy, and cybersecurity law. Paul also teaches Privacy Compliance at UC Law San Francisco (Formerly UC Hastings). He regularly publishes and speaks on privacy and tech topics, and is CIPP/A, CIPP/C, CIPP/E, CIPP/US, CIPM, CIPT and FIP certified.

1. Judgment of the Court (Grand Chamber) of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Request for a preliminary ruling from the High Court (Ireland): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

2. EU Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, 4 June 2021: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

3. Data Protection Commission announces conclusion of inquiry into Meta Ireland, Press Release, https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland

4. European Data Protection Board, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Version 2.0, Adopted on 14 February 2023, available at: https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

5. Paragraph 18, *Guidelines 05/2021*

6. Paragraph 21, *Guidelines 05/2021*

7. Paragraph 16, *Guidelines 05/2021*

8. Paragraph 27, *Guidelines 05/2021*

9. See the EDPB's *Guidelines 04/2021 on Codes of Conduct as tools for transfers*

10. See the EDPB's *Guidelines 07/2022 on Certification as a tool for transfers*

11. See the EDPB's *Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*

12. Irish Data Protection Commission, *In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited), Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation*, DPC Inquiry Reference IN-20-8-1: https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf

13. EU Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, 4 June 2021: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

14. Executive Order 14086 of October 7, 2022, *Enhancing Safeguards for United States Signals Intelligence Activities*: https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

15. European Commission, Press Corner, *Questions & Answers: EU-U.S. Data Privacy Framework*, 7 October 2022, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

16. EU Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, 10 July 2023: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

17. European Commission, Press Corner, *Questions & Answers: EU-U.S. Data Privacy Framework*, 7 October 2022, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

18. European Commission, Press Corner, *Questions & Answers: EU-U.S. Data Privacy Framework*, 7 October 2022, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION
400 Capitol Mall, Suite 650
Sacramento CA, 95814