Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code, and insert it in the pop-up survey that will appear in a new browser tab after you exit out of this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.

Audio

The audio will remain quiet until we begin at 11:00 am ET.

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

Morgan Lewis

TECHNOLOGY MARATHON

AI and Data Privacy : US and European Privacy Laws

May 18, 2023

Presenters

Ezra D. Church

Pulina Whitaker

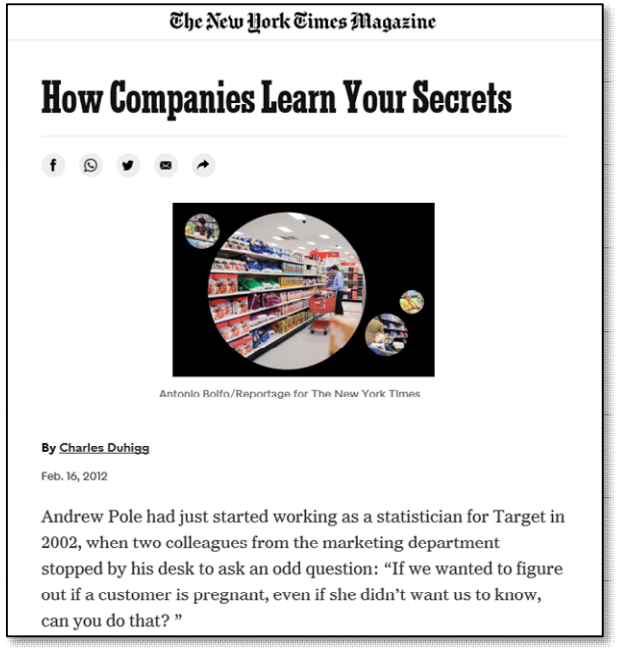
Morgan Lewis

Overview

- AI and Privacy – A privacy collision course?
- Privacy Rights – Can they be protected?
- Anonymization – What does it really mean?
- Data Acquisition - Privacy policies, lawful processing and contracts
- Security Measures

AI and Privacy – A Privacy Collision Course?

- Many of the most interesting data sets are those with lots of personal information
- AI magnifies the ability to analyze personal information in ways that may intrude on privacy interests
- Legal problems arise when AI projects fail to account for legal protections for privacy
- Business problems arise when people lose trust in AI
- To avoid legal trouble and ensure public trust, AI must take privacy interests into account



The New York Times Magazine

How Companies Learn Your Secrets

Antonio Bolfo/Reportage for The New York Times

By Charles Duhigg

Feb. 16, 2012

Andrew Pole had just started working as a statistician for Target in 2002, when two colleagues from the marketing department stopped by his desk to ask an odd question: "If we wanted to figure out if a customer is pregnant, even if she didn't want us to know, can you do that? "

AI and Privacy—Two Types of Concerns

- Input Concerns
  - Typically, AI depends on huge data sets that can include personal information subject to data privacy laws.
  - Is there consent or another justification for use in this way?
  - Can the personal information be used in a way that is consistent with privacy rights, such as deletion?
  - Will reasonable information security be maintained?
- Output Concerns
  - Is AI being used to arrive at conclusions that raise privacy concerns?
  - Is it being used to make decisions that impact privacy and other rights, potentially unfairly / bias?
  - Do people understand how the technology is used and how it might impact them?

AI and Privacy Rights

Morgan Lewis

Europe v. US Privacy Regimes

GDPR

- One fairly comprehensive privacy law in the EU and UK
- Industry-agnostic
- All personal data, regardless of type or context
- Biometric data is a "special category of data" – restricted processing conditions
- Automated processing of data is tightly regulated

US Privacy law

Money: Gramm-Leach-Bliley Act etc.

Health: HIPAA

Kids: COPPA, FERPA, state laws

State Consumer Privacy Laws

Others! Biometrics, state security regulations etc.

The General Data Protection Regulation – in EU and UK

- The GDPR applies across Europe and the UK.
- The GDPR applies to processors and controllers having an EU/UK-based establishment where personal data are processed in the context of the activities of this establishment.
- The GDPR also applies to controllers and processors based outside of the EU/UK territory where the processing of personal data regarding EU data subjects relates to:

  - the offering of goods or services (regardless of payment); and/or

  - the monitoring of data subjects' behavior within the EU/UK.

- "**Personal Data**" means any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The General Data Protection Regulation cont'd

- Right to request to be forgotten, have data rectified or deleted
- *Privacy by design:* privacy safeguarding technology built-in from the start
- Actively factor privacy considerations into the design and upgrade of all systems, policies, settings which process personal data
- *Privacy by default:* privacy-friendly default settings until user chooses otherwise
- Data protection impact assessment: prior to processing if high risk for individuals
- Notify data breach to DPA without undue delay/within 72 hours and to individuals without undue delay if there is likely to be high risk to individuals

The General Data Protection Regulation (cont.)

- Article 22 covers "automated individual decision-making, include profiling."
- Data subject has the right to object unless:
  - Necessary to entering or performing a contract between data subject and controller
  - Authorized by law governing controller and which lays down adequate safeguards for the data subject rights and freedoms and legitimate interests
  - Data subject provides explicit consent
- No processing of the special categories of data, including biometric data, unless there is explicit consent, or the processing is in the public interest and suitable measures to safeguard the data subjects' rights and freedoms and legitimate interests are in place.
- For AI: lawfulness, fairness and transparency are key requirements.

AI Ethics Framework Proposal

- It remains a hot topic for Europe and AI is in the sights of supervisory authorities.
- EU Commission passed a vote in October 2020 for an ethics framework governing AI and privacy so future laws should be made in line with the following guiding principles:
  - a human-centric and human-made AI;
  - safety, transparency and accountability;
  - safeguards against bias and discrimination;
  - right to redress;
  - social and environmental responsibility; and
  - respect for privacy and data protection.
- High-risk technologies should allow for human oversight at any time so if the AI has a self-learning ability that may be dangerous and that may breach ethical principles, humans should be able to disable this function, to restore control back to humans.

EU Coordinated Plan for AI

- On 21 April 2021, the European Commission proposed new rules and actions in an effort to turn Europe into a global hub for 'trustworthy' AI. This is a wide-reaching standard aimed at both harmonising the ethical use of AI and strengthening AI's position in the EU.
- The EU's proposals consist of the first legal framework on AI (the "*AI Act*") and a coordinated plan ("*Coordinated Plan*") specifically aimed at guaranteeing the safety and fundamental rights of people and businesses whilst simultaneously strengthening AI innovation across the EU.
- The EU's emphasis is on ensuring that developments of new global norms, led by the EU, can be trusted. The new AI Act is intended to ensure that Europeans are able to trust AI powered technology.
- The Coordinated Plan provides an outline of the necessary policy changes and investment amongst Members States to bolster Europe's position in developing a human-centric, sustainable, trustworthy and secure AI.
- In 2022, the UK announced a 10 year plan to make the UK an "*AI Superpower*" in its National AI Strategy (National AI Strategy - HTML version - GOV.UK (www.gov.uk)).

Prohibited AI Systems

- Certain AI systems are prohibited under the AI Act, including those that:
  - Deploy subliminal techniques beyond a person's consciousness to materially distort the person's behaviour and cause harm;
  - Exploit any of the vulnerabilities of a specific group of persons to materially distort the person's behaviour and cause harm;
  - Evaluate/classify the trustworthiness of natural persons, i.e., social scoring; and
  - Use "real-time" remote biometric identification systems in publicly accessible spaces for law enforcement.
  - The European Parliament's current proposals expand the scope of prohibited AI systems to include:
    - AI systems capable of "*assess[ing] the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons*"; and
    - AI systems "*that create or expand facial recognition databases through the untargeted scraping of facial images from social media profiles or CCTV footage.*"

The UK

- The AI Act no longer applies to the UK, yet it is still relevant to UK businesses as a result of its extra-territorial reach.
- From a privacy perspective, the UK needs to maintain data protection equivalence with the EU to maintain its adequacy status – up for review by December 2024.
- On 29 March 2023, the UK government published its White Paper "*A pro-innovation approach to AI Act"* setting out the UK government's framework and approach to the regulation of AI.
- The UK government has decided to support existing regulators (the ICO, the CMA, the FCA, Ofcome, the HSE and the Human Rights Commission) and develop a sector-focused and principles-based approach rather than giving responsibility to a new single regulator.
- UK regulators are expected to publish non-statutory guidance that is in the next 12 months and is expected to include practical tools, risk assessment templates and standards to set out how to implement the five principles to facilitate the safe and innovative use of AI, including: (i) safety, security and robustness; (ii) transparency and explainability; (iii) fairness; (iv) accountability and governance; (v) contestability and redress.

UK White Paper on AI: a pro-innovation approach to AI Act

- The Department for Science, Innovation and Technology (DSIT) published the long-awaited AI white paper on 29 March 2023.
- The white paper provides a framework to guide the UK's approach to regulating AI. It provides a cross-sectoral, principles-based framework to increase public trust in AI and develop capabilities in AI technology, including expertise in foundation models for generative AI. The announcement includes a sandbox trial for the development and testing of new products.
- The white paper sets out five principles which regulators must consider to build trust and provide clarity for innovation, as follows:
  - Safety, security and robustness.
  - Transparency and explainability.
  - Fairness.
  - Accountability and governance.
  - Contestability and redress.
- UK regulators will incorporate these principles into guidance to be issued over the next 12 months. Risk assessment templates and other tools will also be issued, including assurance techniques, voluntary guidance and standards.

UK White Paper on AI: a pro-innovation approach to AI Act (cont'd)

- The government has identified that the regulatory regime must display the following characteristics: pro-innovation, proportionate, trustworthy, adaptable, clear and collaborative. The regulators are tasked with developing guidelines which support this. These traits underpin the four key elements for the AI framework which the government hopes will promote a coherent regulatory approach which the regulators must work towards. The four elements are:
  - Defining AI based on its unique characteristics to support regulator co-ordination.
  - Adopting a context-specific approach.
  - Providing a set of cross-sectoral principles to guide regulator responses to AI risks and opportunities. Regulators will initially be free to apply these principles to meet the needs of their sectors but the government anticipates introducing a statutory duty requiring regulators to have due regard to the principles following expiry of the initial non-statutory implementation period and when parliamentary time allows.
  - Delivering new central government functions to support regulators in their delivery of the AI regulatory framework and the benefits of horizon scanning and an iterative regulatory approach.
  - Annex A of the AI white paper summarises the factors that regulators may wish to consider when creating their guidance, broken down by the five principles of the AI framework.

Information Commissioner's Guidance

- On 11 April 2023, the ICO issues its response to the Government's consultation on the White Paper, stating its recognition of the importance of AI to UK's prosperity and providing "*transformational potential*" to improve lives and livelihoods.
- The ICO also recognises AI's relationship with personal data and therefore as the data protection authority in the UK, an equal recognition of its own "c*entral role in the governance of AI".*
- In the response, the ICO makes it clear that the proposals in Government's White Paper will incur costs, to cross-economy regulators such as the ICO with a need to produce products suitable for different sectors in conjunction with other regulators. As such, the ICO welcomes "*further discussions with government on the funding required to enable these proposals to succeed".*
- The ICO has published detailed guidance on AI and data protection, updated on 15 March 2023.
- In 2022, the ICO also issued its toolkit which acts as a practical checklist of the key data protection issues that need to be considered by organisations from the outset of any project that they are planning. The ICO acknowledges that the toolkit is not "a *pathway to absolute compliance with data protection law*" - but is a strong starting point.

CHATGPT and the Italian Data Protection Authority

At the end of March this year, the Italian Data Protection Authority, the Garante, issued a temporary ban on Open AI LLC to temporarily stop ChatGPT's processing of individuals' personal data in Italy pending the supervisory authority's investigation into ChatGPT's privacy practices.

- The data protection authority had particular concerns about the lack of transparency in the handling of user data.

The block on OpenAI's ChatGPT has now been lifted.

- Given *"improved transparency and rights for European users"* e.g., users now have the option to object to the storage of chats in the chat history.

This was first action of its kind taken by a data protection authority in the EU in connection with ChatGPT's data processing.

- Rapid development of ChatGPT has attracted legislators and regulators all over Europe.

The action is of particular interest given the context of data processing e.g., in using and 'training' machine learning software.

- There is discussion on whether AI systems such as ChatGPT should be classified as high-risk AI systems although at present,it would only receive this classification if the system also posed a significant risk to health, safety or fundamental rights.

US Regulation / Guidance on AI

- Sector specific laws apply!
- Blueprint for an AI Bill of Rights (Oct. 2022)
  - White House Office of Science and Technology Policy (OSTP)
  - Five principles to help guide the design, use and deployment of AI systems
    - Safe and effective systems
    - Algorithmic discrimination protections
    - *Data privacy*
    - Notice and explanation
    - Human alternatives, consideration, and fallback

US Regulation / Guidance on AI

- National Institute of Standards and Technology (NIST) to develop the AI Risk Management Framework (AI RMF), Jan. 26, 2023
  - Specifically identifies privacy as a risk:
    - "Some risks related to AI systems are common across other types of software development and deployment. Examples of overlapping risks include: privacy concerns related to the use of underlying data to train AI systems; the energy and environmental implications associated with resource-heavy computing demands; security concerns related to the confidentiality, integrity, and availability of the system and its training and output data; and general security of the underlying software and hardware for AI systems."
    - "Privacy values such as anonymity, confidentiality, and control generally should guide choices for AI system design, development, and deployment. Privacy-related risks may influence security, bias, and transparency and come with tradeoffs with these other characteristics. Like safety and security, specific technical features of an AI system may promote or reduce privacy. AI systems can also present new risks to privacy by allowing inference to identify individuals or previously private information about individuals."
    - "Privacy risk due to enhanced data aggregation capability for AI systems."

FTC Enforcement Actions

- FTC has issued a series of reports on AI and related consumer and privacy issues, w/ most recent on April 19, 2021
  - Be transparent with consumers about how you use automated tools (e.g., FTC's WW Settlement)
  - Be transparent when collecting sensitive data (e.g., FTC's Everalbum Complaint, facial recognition)
  - Look out for automated decisions, which can prejudice unfairly and raised issues under the FCRA
  - Decisions based on algorithms must be explained to customers / consumers
  - Algorithmic disgorgement! (Weight Watchers, Everalbum, and Cambridge Analytica)

California Consumer Privacy Act (CCPA)

- California passed into law the California Consumer Privacy Act (CCPA) on March 28, 2019, enforced starting July 1, 2020, included a broad definition of "personal information" and new privacy rights.
- California Privacy Rights Act (amends CCPA), includes a number of provisions that speak more directly to AI, including a definition of "profiling" and rules about "automated decision making."
- Similar rules enacted in the Virginia Consumer Data Protection Act (eff. Jan. 1. 2023), the Colorado Privacy Act (eff. July 1, 2023), and Connecticut Data Privacy Act (July 1, 2023).
- Impact both privacy input and privacy output risks

CCPA Overview (cont.)

- Requirements around Personal Information (PI) include:
  - Notice about collection and use of PI
  - Responding to Requests. Four types:
    - To Know Categories of PI
    - To Know Specific Pieces of PI
    - To Correct inaccurate information
    - To Delete PI
    - To Opt Out of Sale of PI (any transfer to third party for monetary or other consideration)
  - No discrimination or retaliation for exercising rights

Very Broad Definition of "Personal Information"

- Personal information includes any information that "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
  - Much broader than the definition of personal information under CA's security breach notification law and historic definitions in US
  - More like GDPR
- Extremely broad definition intended to include the sort of robust consumer profile and preference data collected by social media companies and online advertisers

CCPA Definition of Personal Information

1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) ***Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes***

State Law Regulation of Automated Decision Making

- CCPA (as amended by CPRA) will impact "profiling" and "automated decision-making"
  - "Profiling" means any form of automated processing of personal information, . . . to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
  - Requires a data privacy impact assessment for processing activities including profiling
  - Requires the California Privacy Protection Agency (CPPA) to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those processes, as well as a description about the likely outcome of the process with respect to the consumer."
  - CPPA is currently involved in "pre rulemaking activities" and has held a series of meetings and requested public comment, with the period closed March 2023.
- VCDPA, allows individuals to opt out of "profiling in furtherance of decisions that produce legal or similarly significant effects" and requires a DPIA for these activities (like CCPA)
- Colorado, Connecticut and other state laws have similar requirements

Your CLE Credit Information

For ALL attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

THE CLE CODE IS:

RZC8745

Anonymization

Morgan Lewis

Anonymization / Deidentification

- Privacy laws focus on personal information—if you can do AI without personal information, most of the privacy issues evaporate
- GDPR: Anonymisation/Pseudonymisation distinction
  - **Anonymisation** is the process of permanently removing personal identifiers that could lead to an individual being identified
  - **Pseudonymisation** is a technique that replaces or removes information in a data set that identifies an individual, but it can be re-identified
- US CCPA: Under "Personal Information" does not including "consumer information that is deidentified or aggregate consumer information."
  - **Deidentified data**: Information that "cannot reasonable identify, relate to, describe, be capable of being associated with, or be linked directly or indirectly to a particular consumer."
    - Must have technical safeguards to prevent reidentification
  - **Aggregate data**: "Information that relates to a group or category of consumers, from which individual identities have been removed, that is not linked or reasonably linkable to any consumer or household."
  - **Publicly available**: Information that is lawfully made available from federal, state, or local government records.
- So, is it a solution?

Data Acquisition for AI - Privacy Policies and Contracts

Morgan Lewis

Privacy Policies - US

- GDPR / FTC / and State Laws (e.g., CA, NV & DE)
- Self-imposed regulation
- Basic principles
  - What information is collected
  - How it is collected
  - Purpose of collection
  - To whom is it shared
  - Choices and rights
- Must notify regarding material, retroactive changes
- Other public statements about privacy and security?

Privacy Notices - GDPR

- GDPR includes mandatory transparency obligations
- Privacy policy or notice provided by controllers (only):
  - the identity and contact details of the data controller and where applicable, the data controller's representative) and the data protection officer
  - the purpose of the processing and the legal basis for the processing
  - the legitimate interests of the controller or third party, where applicable
  - the categories of personal data
  - any recipient or categories of recipients of the personal data
  - the details of transfers to third country (e.g. to US) and method of transfer such as model clauses or other data transfer agreements
  - the retention period
  - the data subject's rights relating to the processing such as the right of access and rectification
  - the right to withdraw consent at any time, where relevant
  - the right to lodge a complaint with a supervisory authority
  - the source of the personal data and whether it came from publicly accessible source
  - whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
  - the existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences

Contracts

- Often data will come from another source, in which case there are often contract requirements that also may impact use of data for AI
- Confidentiality clauses
- Privacy clauses
- Data use / rights language
- Data protection addendums, exhibits
- Retention requirements
- Breach notice obligations
- California: acquisition of data for AI may be a “sale”

Processing Agreements - GDPR

- Processors must execute processing agreements with controllers under Article 28:
  - Specify categories of data and data subjects
  - Follow controller's instructions
  - Duties of confidentiality
  - Security of processing obligations
  - Assist controller with GDPR compliance
  - Restrictions on engaging sub-processors and data transfers
  - Assist controller with subject rights (access, deletion etc)
  - Notify controller of data breach
  - Return/delete data on termination
  - Controller right of audit
- NB: direct liability for processors and for failure to have a DPA (recent CNIL fine of EUR 1.5m).

Data Security

Morgan Lewis

Data Security

- US Sector-specific laws may apply; state laws require reasonable security
- MA Security Regulations
  - Have a written information security plan
  - Additional administrative discipline
  - Social security numbers
  - Encryption
  - Training
- GDPR requirement for technical and organisational measures to protect personal data
- Contracts may require certain security standards – NB GDPR data processing agreements must include security obligations


Questions?
Morgan Lewis

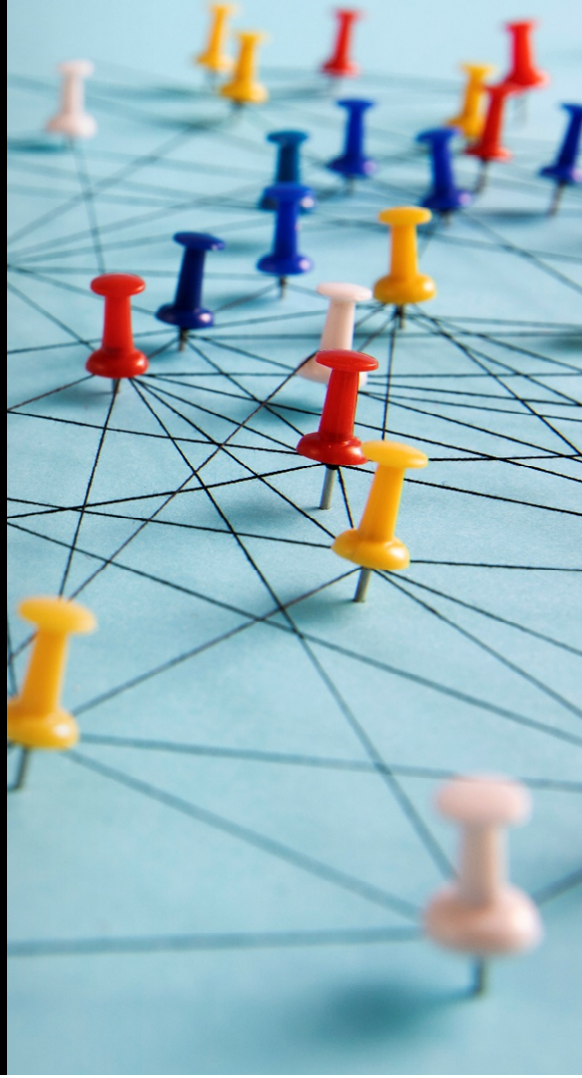
Ukraine Conflict Resources

Our lawyers have long been trusted advisers to clients navigating the complex and quickly changing global framework of international sanctions. Because companies must closely monitor evolving government guidance to understand what changes need to be made to their global operations to maintain business continuity, we offer a centralized portal to share our insights and analyses.

Morgan Lewis

To help keep you on top of developments as they unfold, visit the website at **www.morganlewis.com/topics/ukraine-conflict**

To receive a daily digest of all updates, please visit the resource page to **subscribe** using the "Stay Up to Date" button.



EZRA D. CHURCH

Ezra D. Church
Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

Ezra D. Church counsels and defends companies in privacy, cybersecurity, and other consumer protection matters. He helps clients manage data security and other crisis incidents and represents them in high-profile privacy and other class actions. Focused particularly on retail, ecommerce, and other consumer-facing firms, his practice is at the forefront of issues such as biometrics, artificial intelligence, location tracking, ad tech, and blockchain. Ezra is a Certified Information Privacy Professional (CIPP) and co-chair of the firm's Class Action Working Group.

PULINA WHITAKER

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

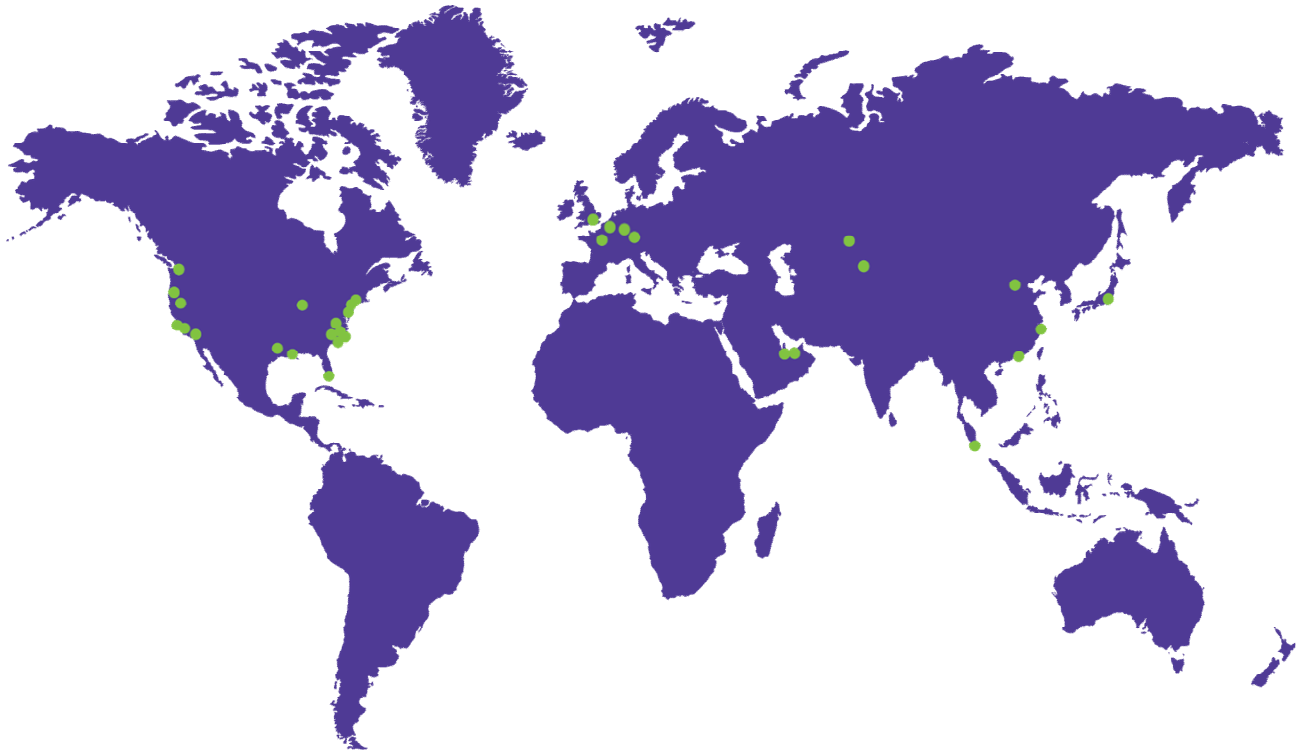
Pulina Whitaker's practice encompasses data privacy and cybersecurity as well as employment matters. She is a co-head of the firm's global privacy and cybersecurity practice and has extensive cross-border experience for over 20 years working with international and European clients to help them comply with European and other international privacy laws, including the EU and UK General Data Protection Regulation, including advising on privacy collection and processing requirements, audits of data processing activities and data security incidents.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU