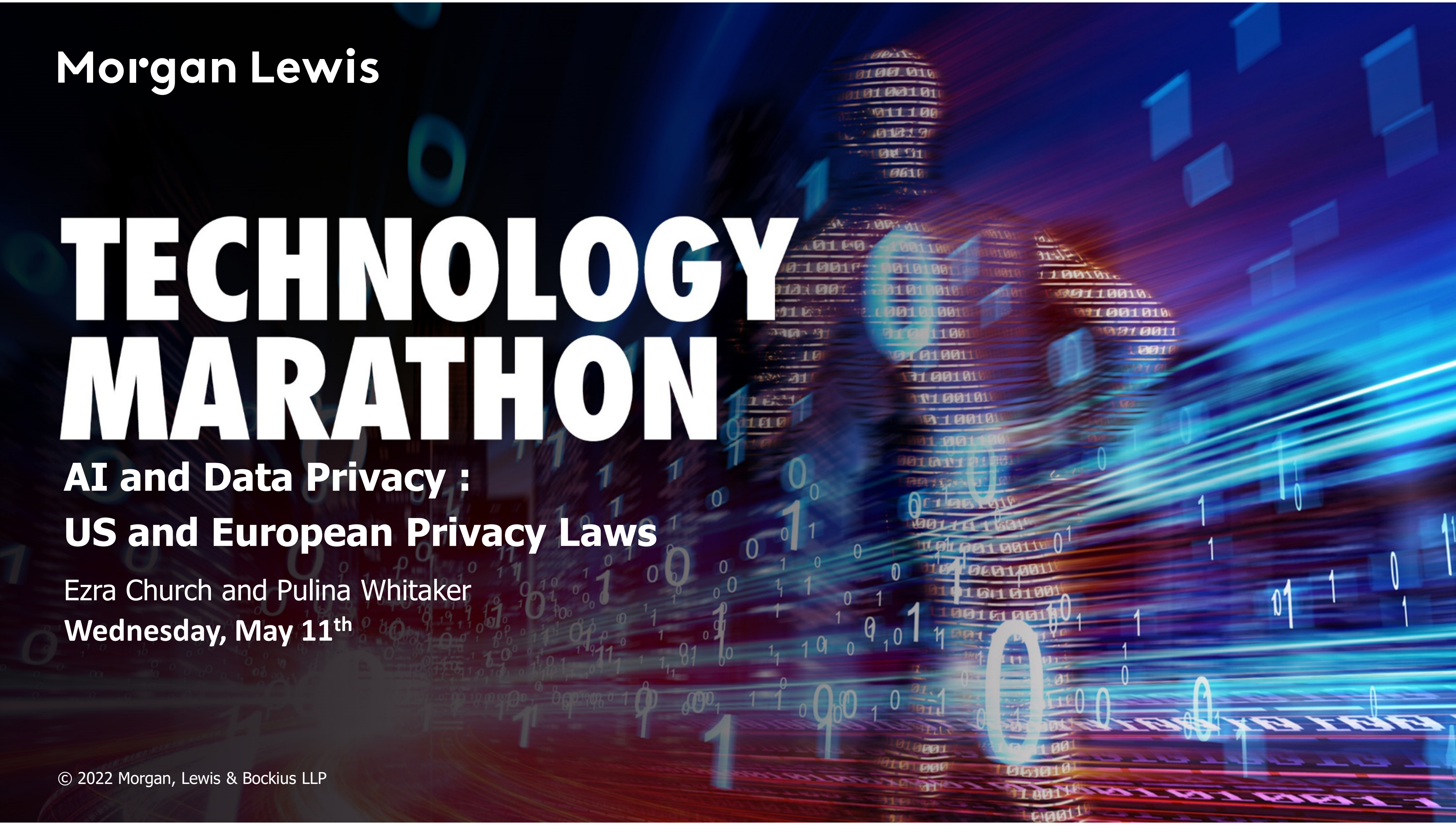


Morgan Lewis

TECHNOLOGY MARATHON

AI and Data Privacy :

US and European Privacy Laws

Ezra Church and Pulina Whitaker

Wednesday, May 11th

Presenters

Ezra D. Church

Pulina Whitaker

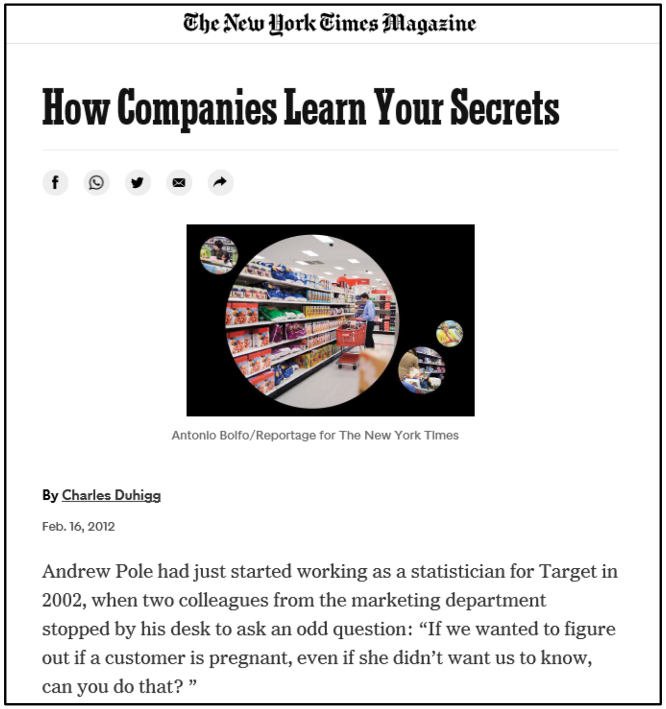
Morgan Lewis

Overview

- AI and Privacy – A Collision Course?
- Privacy Rights
- Anonymization
- Data Acquisition - Privacy Policies, Lawful Processing and Contracts
- Security Measures

AI and Privacy – A Collision Course?

- AI magnifies the ability to analyze personal information in ways that may intrude on privacy interests
- Many of the most interesting data sets are those with lots of personal information
- 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 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

California: CCPA / CPRA

Others! Biometrics, state security regulations etc.

The General Data Protection Regulation – in EU and UK

- The GDPR now implemented in the UK and applies across Europe.
- 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 <u>outside</u> 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 covered “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 is a hot topic for Europe.
- 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 ("AI Regulation") and a new 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 Regulation is intended to ensure that Europeans are able to trust AI.
- 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.
- The UK has 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)).

AI System

- EU defines “AI System” rather than AI:

  “artificial intelligence system” (AI system) means a system that:

  (i) receives machine and/or human-based data and inputs,

  (ii) infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling implemented with the techniques and approaches listed in Annex I [of the Proposal for an AI Act], and

  (iii) generates outputs in the form of content (generative AI systems), predictions, recommendations or decisions, which influence the environments it interacts with.”

The first legal framework on AI

- In April 2018, many European countries, including the UK, signed a Declaration of co-operation on Artificial Intelligence (AI) and launched a plan. 3 years later, the Commission has published the first-ever legal framework on AI in its proposed *"Regulation Laying Down Harmonized Rules on Artificial Intelligence":*

The definition of AI systems is wide in scope:

"software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

Annex I includes machine learning approaches, logic, knowledge-based and statistical approaches.

The proposed AI Regulation applies to:

i) providers of AI systems in the EU;
ii) users of AI systems located within the EU; and
iii) providers and users of AI systems that are located outside the EU if the output produced by the system is within the EU.

The following AI systems are identified as "*high-risk":*

(i) Safety components of products (such as toys, machinery, medical devices); and
(ii) Systems used to evaluate creditworthiness, biometric identification and critical infrastructure.

The first legal framework on AI

- Certain AI systems are prohibited under the AI Regulation, 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 UK

- The AI Regulation no longer applies to the UK, yet it is still relevant to UK businesses as a result of its extra-territorial reach.
- The UK has now published its 10 year strategy on AI, and the government has confirmed that "*unleashing the power of AI is a top priority in our plan to be the most pro-tech government ever*" and plans to turn the UK into an "*AI Superpower*".
- From a privacy perspective, the UK needs to maintain data protection equivalence with the UK to maintain its adequacy status – up for review by December 2024.
- The Queen's Speech yesterday included a proposal for a Data Reform Bill which has not yet been published – but may include some changes to privacy legislation.

Information Commissioner's Guidance

- In July 2020, the ICO issued a framework for auditing impact of AI comprising:
  - auditing tools and procedures that ICO will use in audits and investigations;
  - The ICO detailed guidance on AI and data protection; and
  - a toolkit designed to provide further practical support to organisations auditing the compliance of their own AI systems.
- Last year the ICO 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.
- The ICO published a paper in August 2021 in which it provides its support to the Commission's proposals on artificial intelligence and the AIA. It has also published guidance on AI and data protection (https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/).
- In conjunction with the Alan Turing Institute, it has also published guidance on explaining AI decisions.

FTC Guidance on AI

- FTC has issued a series of reports on AI and related consumer and privacy issues, with report with 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

Other Federal Action on AI

- As part of the National Defense Authorization Act for 2021, Congress required the National Institute of Standards and Technology (NIST) to develop the AI Risk Management Framework (AI RMF).
  - Initial draft issued for comment, w/ comment period ended April 29.
  - Specifically identifies privacy as a risk:

"Like safety and security, specific technical features of an AI system may promote privacy, and assessors can identify how the processing of data could create privacy-related problems."

State and Local Laws on Artificial Inteligence

- Bills or resolutions introduced in at least 17 states in 2021, enacted in Alabama, Colorado, Illinois and Mississippi.
  - Alabama: Established counsel to review issue and advise the government on use and development of AI
  - Colorado: Prohibits insurers from using external consumer data in a way that unfairly discriminates.
  - Illinois: Amends the AI Video Interview Act, requires disclosure and consent and reporting data to the state government.
  - Mississippi: Requires instruction on AI and machine learning in K-12 curriculum.
  - NYC: Prohibits use of AI tools in employment decisions unless it has been subject to a "bias audit" and use is disclosed, with opportunity to request alternative process.

California Consumer Privacy Act (CCPA)

- California passed into law the California Consumer Privacy Act (CCPA) on March 28, 2019.
- The law started on January 1, 2020.
- Enforcement began July 1, 2020.
- Failure to comply could result in significant penalties and reputational harm.

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 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
  - Under CPRA, starting January 1, 2023, cannot retain personal information for longer than reasonably necessary for the stated purpose for which it was collected

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***

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?

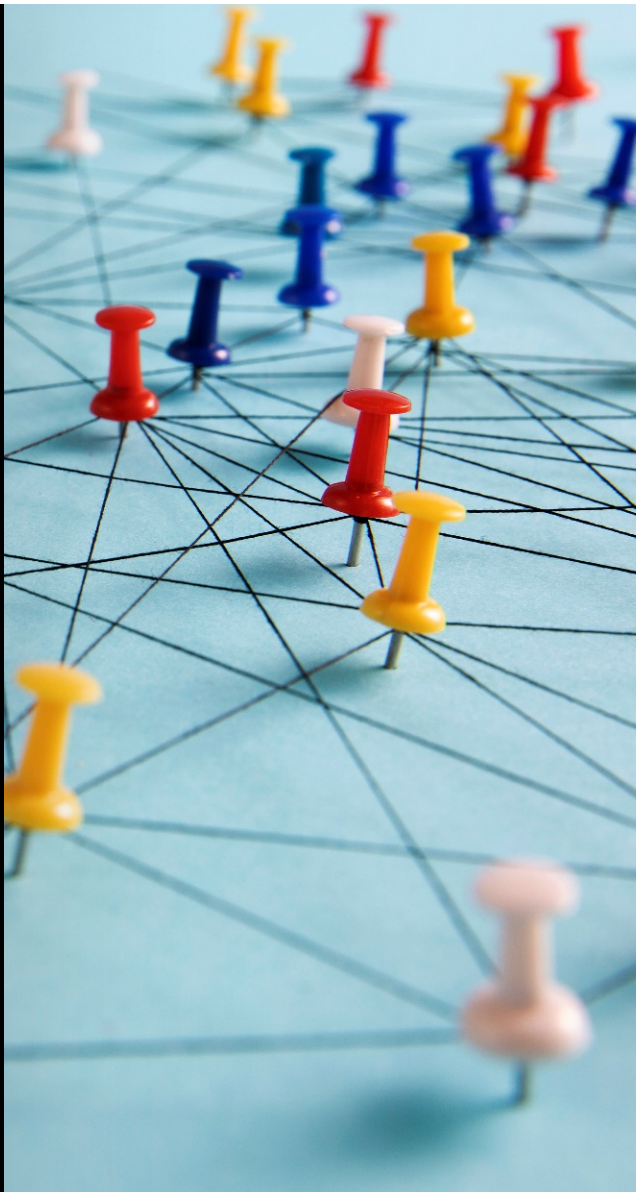
Ukraine Conflict Resources

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.

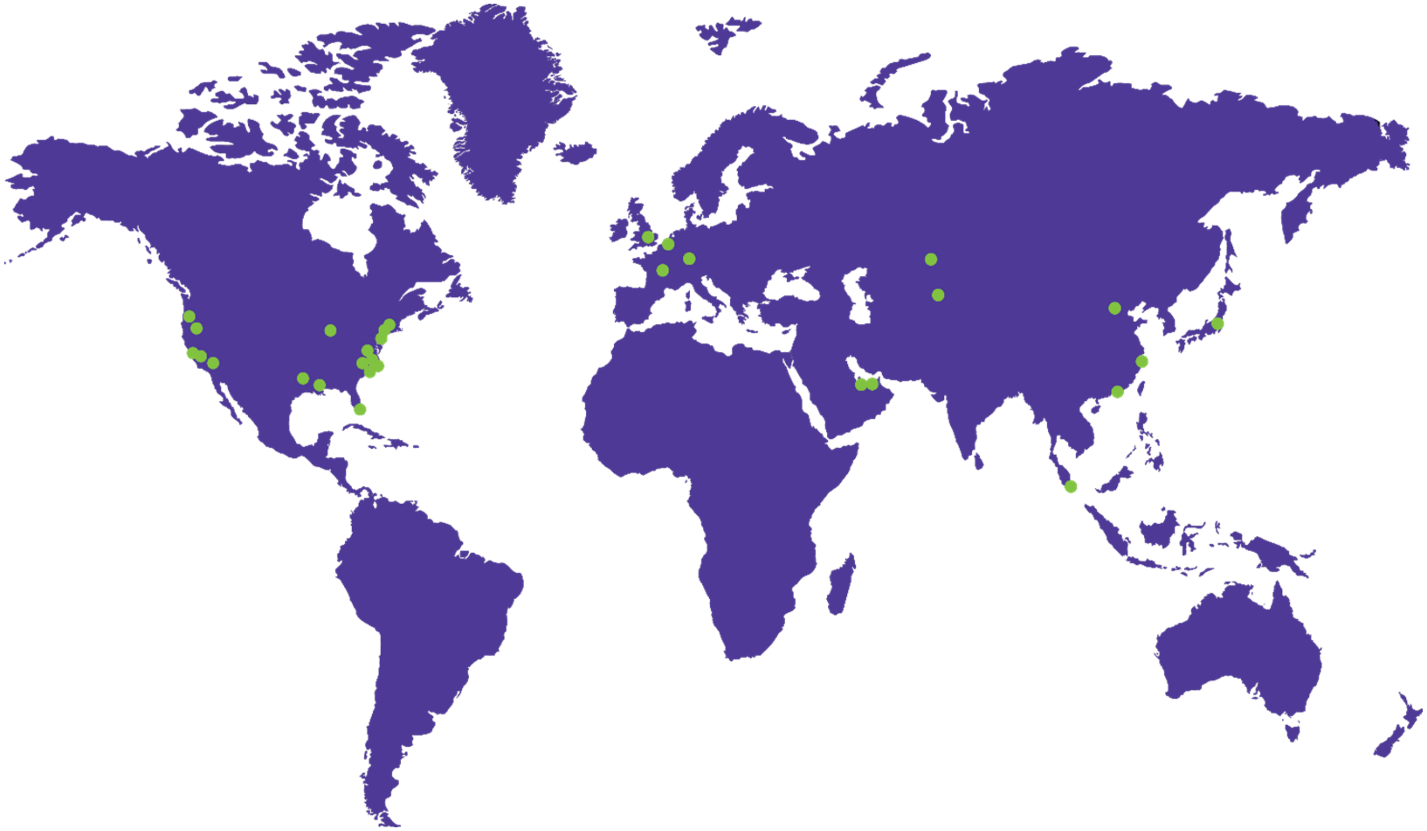
She has been described by clients in The Legal 500 as "extremely knowledgeable with a practical approach" and is noted as being "a key name for issues covering employment and data privacy work." Also named as a Legal 500 leading practitioner, they go on to note Pulina "is head and shoulders above the data protection and privacy pack on her command of law, requirements, and implementation."

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.