



Morgan Lewis

SILICON VALLEY **FIRST CUP OF COFFEE** SEMINAR SERIES

UPCOMING SEMINARS:

Artificial Intelligence (AI) Boot Camp

- | | |
|------------|---|
| January 12 | Computer-Implemented Inventions in Biotechnology and Healthcare, Patentability from European and US Perspective |
| January 13 | M&A and Investment into AI Companies |
| January 19 | Software As a Medical Device: US FDA Regulatory and Legal Framework |
| January 20 | Patent and Trade Secret Protection for Inventions That Use AI |
| January 21 | AI in Hiring and Recruiting |
| January 28 | AI and Copyright |



Morgan Lewis

SILICON VALLEY FIRST CUP OF COFFEE SEMINAR SERIES

UPCOMING SEMINARS:

Artificial Intelligence (AI) Boot Camp

- | | |
|-------------|--|
| February 2 | The Ethics of Artificial Intelligence for the Legal Profession |
| February 3 | AI and Data Privacy |
| February 4 | Patents for MedTech AI: Opportunities and Pitfalls |
| February 9 | IP Landscape of AI Hardware Startups |
| February 10 | The Risks of Bias and Errors in AI-Enabled Decision-Making |
| February 11 | AI in Digital Advisory Offerings: Regulatory Considerations |
| February 16 | Bias Issues and AI |

Morgan Lewis

AI AND DATA PRIVACY

**Pulina Whitaker, Ezra D. Church
and Andrew J. Gray IV**

February 3, 2021

Presenters



Pulina Whitaker



Ezra D. Church



Andrew J. Gray IV

Morgan Lewis

Overview

- AI and Privacy—Collision Course
- Privacy Rights
- Anonymization
- Collecting Data—Privacy Policies and Contracts
- Security practices

AI and Privacy—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

f WhatsApp Twitter Email Share




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



AI

Morgan Lewis

EU v. US Privacy Regimes

GDPR

- One comprehensive privacy law
- All industries
- All personal data, regardless of type or context
- Biometric data is a “special category of data” – restricted processing conditions

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 EU General Data Protection Regulation

- The GDPR replaced EU Data Protection Directive for commercial data privacy obligations in Europe.
- Expanded application of the EU data privacy obligations.
- The GDPR applies to processors and controllers having an EU-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 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.
- “**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 EU 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 EU 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.

European Commission Strategy on AI

- Proposal for a Regulation on Data Governance (Data Governance Act) – November 2020, addressing:
 - Making public sector data available for re-use, in situations where such data is subject to rights of others;
 - Sharing of data among businesses, against remuneration in any form;
 - Allowing personal data to be used with the help of a “personal data-sharing intermediary” designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR); and
 - Allowing data use on altruistic grounds.
- Strategy on AI is aimed to:
 - place Europe ahead of technological developments and encourage the uptake of AI by the public and private sectors;
 - prepare for socio-economic changes brought about by AI; and
 - Ensure Europe has an appropriate ethical and legal framework.

European Co-ordination

- Many European countries, including the UK, have signed a Declaration of co-operation on Artificial Intelligence (AI).
- Legislative proposal expected the first quarter of 2021.
- ICO has 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.

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

AI

Morgan Lewis

Anonymization / Deidentification

- Privacy laws focus on personal information—if you can do AI without personal information, most of the privacy issues evaporate
- EU 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 irectly 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?

Collecting Data 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
 - Notice
 - Access and Control
 - Purpose of collection
- Must notify regarding material, retroactive changes
- Other public statements about privacy and security?

Privacy Notices—EU

- 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. 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”

Data Security



AI

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 EU data processing agreements must include security obligations

Questions?

Morgan Lewis



Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at

[www.morganlewis.com/
topics/coronavirus-
covid-19](http://www.morganlewis.com/topics/coronavirus-covid-19)

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to [subscribe](#) using the purple “Stay Up to Date” button.



Biography



Pulina Whitaker

London

+1.44.20.3201.5550

pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses data privacy and cybersecurity as well as employment. She is a co-head of our global Privacy & Cybersecurity practice. She manages employment and data privacy issues in sales and acquisitions, commercial outsourcings and restructurings. Pulina provides day-to-day advisory support for multinationals on the full spectrum of data privacy issues, including data breaches, data protection compliance issues and data sharing and data transfer arrangements. Pulina has deep experience managing international employee misconduct investigations as well as cross-border data breach investigations. She has been appointed as a compliance monitor for the UN and for USAID. She is also a trustee of Hostage International.

Biography



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.

Biography



Andrew J. Gray IV

Silicon Valley

+1.650.843.7575

andrew.gray@morganlewis.com

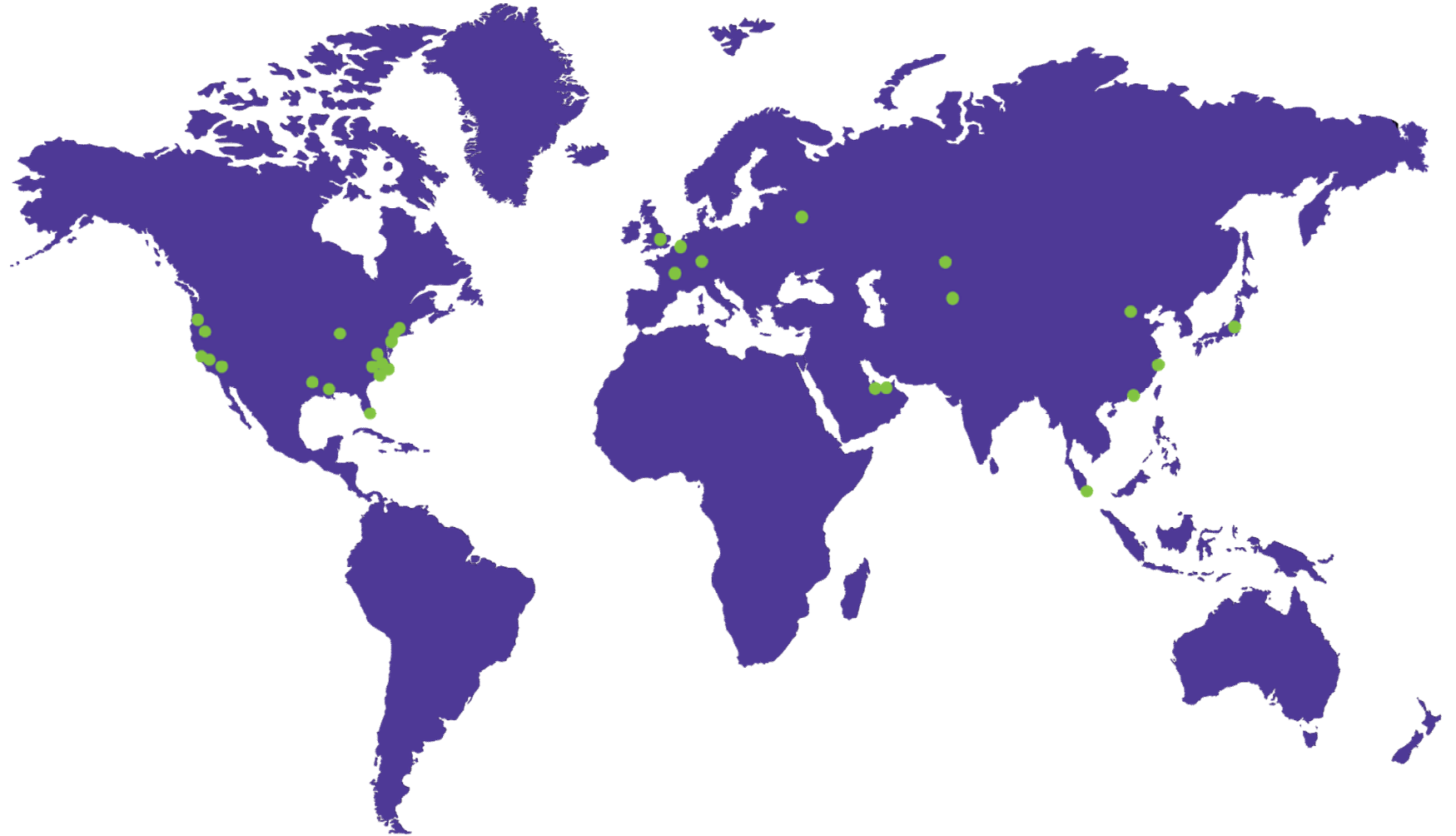
Serving as the leader of Morgan Lewis's semiconductor practice and as a member of the firm's fintech and technology practices, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on Blockchain, cryptocurrency, computer, and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, before the US Patent and Trademark Office's Patent Trial and Appeal Board, and before the US International Trade Commission.

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
Moscow
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 operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2021 Morgan, Lewis & Bockius LLP
© 2021 Morgan Lewis Stamford LLC
© 2021 Morgan, Lewis & Bockius UK LLP

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.