407 | From Civil Rights to Cybersecurity: How Racial, Religious and Political Profiling Led to the General Data Protection Regulation (GDPR) and What It Means for You

2018 NAPABA Convention

November 10, 2018

Moderator:

- Mark J. Alagoas, Staff Attorney, McDermott Will & Emery

Speakers:

- Anna Mercado Clark, Partner, Data Security & Privacy Team Leader, Phillips Lytle LLP
- Scott Lee, Special Counsel, Office of Chief Counsel in the Division of Swap Dealer and Intermediary Oversight at the U.S. Commodity Futures Trading Commission
- Al Park, Senior Partner, Control Risks
- Ami Rodrigues, Data Privacy and Cybersecurity Attorney, The Coca-Cola Company

Introduction to Data Privacy Regulation

- Information privacy law or data protection laws prohibit the disclosure or misuse of information about private individuals.
- Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia and Africa, have now adopted comprehensive data protection laws.
- Basic Principles of Data Protection

Civil Rights History of the GDPR

- The GDPR is just the latest example of Europe's caution on privacy rights. This outlook of privacy as a fundamental right is rooted in the disturbing events of WWII.
  - Hitler's rise to power
  - Mass murder of six million Jews
  - Forced sterilization of more than 300,000 to 400,000 Jews
  - Property registry and confiscation
    - Identification
    - Cross-indexing
    - Classification
    - Tracking
    - Transportation

Civil Rights History of the GDPR (Cont'd)

- Increased speed, scope, reliability and efficiency
- Impacted marriages, employment, property ownership
- Tabulating machine
  - Types of punch card data
- By 1937, punch card production was at 74 million per month.
- By 1934, a six-month supply of punch cards could fill 55 railroad cars (produced in the U.S.).
- Cooperation among various agencies (population, local labor, local and regional statistical offices, and State health offices) and search of various other sources (*e.g.*, forced reporting by Jewish communal leaders, Germanic Family Baptismal Registry, church records)

Civil Rights History of the GDPR (Cont'd)

- The European Convention of Human Rights, first considered in 1950 and ratified in 1953, considered the atrocities of the Second World War and how these could be avoided.
- History of "special categories of personal data"
  - Roma (gypsies), homosexuals, Jehovah's Witnesses, political opponents, etc.
  - Approximately 17 million people were killed, with Jewish people constituting the majority group and roughly 2/3 of the European Jewish population.
  - Impact in European countries other than Germany

Civil Rights History of the GDPR (Cont'd)

- 1983 German Census decision (*Volkszählungsurteil*)
- The concept of individual privacy as a fundamental human right continued to be developed in the face of authoritarian regimes, which every continental European country has experienced.
- Should we view the GDPR as protectionist response that is anti-business or relevant to the notion of privacy as a fundamental human right?
  - Consider: the internment of Japanese Americans during WWII, the Rwandan genocide and the latest Rohingya crisis in Burma/Bangladesh, the current President's approach to extreme vetting

So, Why Does GDPR Exist?

- Public concern over privacy
- Europe in general has long had more stringent rules around how companies use the personal data of its citizens.
- The GDPR replaces the EU's Data Protection Directive, which went into effect in 1995. This was well before the internet became the online business hub that it is today. Consequently, the directive is outdated and does not address many ways in which data is stored, collected and transferred today.

Core Principles of the GDPR

- Lawful, fair and transparent processing
- Limitation of purpose, data and storage (privacy by design)
- Data subject rights

QUIZ: Does the GDPR Apply?

Crazy Rich Company has offices in the United States exclusively. They sell power tools to companies located in Lichtenstein, which is not a member of the EU.

Yes ☐ No ☐

Astrid Leong is vacationing in NYC from Paris. She sends emails to Charlie Wu, who is in Paris.

Yes ☐ No ☐

Peik Lin runs a business out of her California apartment, selling rap CDs to anyone who wants to buy one through her website, which tracks only what visitors place in their shopping cart.

Yes ☐ No ☐

Princess Intan, a Malaysian citizen, makes purchases on Chanel.com while in Amsterdam.

Yes ☐ No ☐

Prof. Rachel Chu, a professor located in America, emails with professors at Oxford University in the UK.

Yes ☐ No ☐

Mahjong.com is a company with a single office in Atlanta, Georgia. It does not sell products nor market outside of the United States. Its website is visited by individuals located all over the world. Website visitors cannot provide any information through the website.

Yes ☐ No ☐

Young Enterprises, located in Madrid, Italy, sells chocolate all over the world. It does not use a computer system but, instead, keeps paper records.

Yes ☐ No ☐

QUIZ: Does the GDPR Apply? (Cont'd)

- The GDPR limits processing of personal data "by automated means" or non-automated means if the data "form[s] part of a filing system or is intended to form part of a filing system" to specific circumstances.

Some Important Terms

- Personal data – "Information relating to an identified or identifiable natural person ('data subject')," including name, identification number, location data, biometric data, health and genetic data, racial or ethnic data, political activity and sexual orientation
- Processing – Any operation performed on personal data, including collection, recording, use, transmission or dissemination of such data
- Controller – Person or entity controlling purpose and means of processing personal data
- Processor – Person or entity processing personal data on behalf of a controller

Personal Data Quiz

- Which of this data is personal data?

a name and surname?	**subjective opinions about a person held by that person's co-workers?**
a company registration number?	an Internet Protocol (IP) address?
a home address?	an individual's psychological profile?
an email address such as name.surname@company.com?	anonymised data?
an email address such as info@company.com?	data held by a hospital or doctor, which could be a symbol that uniquely identifies a person?
Passport / identification card number?	data relating to a deceased person?
Photographs?	false information on an individual?
location data (for example the location data function on a mobile phone)?/	a blood sample?

Personal Data Quiz (Cont'd)

- Almost all of it:

a name and surname?	**subjective opinions about a person held by that person's co-workers?**
	an Internet Protocol (IP) address?
a home address?	an individual's psychological profile?
an email address such as name.surname@company.com?	
	data held by a hospital or doctor, which could be a symbol that uniquely identifies a person?
Passport / identification card number?	data relating to a deceased person?
Photographs?	false information on an individual?
location data (for example the location data function on a mobile phone)?/	a blood sample?

The GDPR Applies to...

- A controller or processor established in the European Union ("EU") or European Economic Area ("EEA") that processes personal data "in the context of the activities" of such an establishment, irrespective of whether data processing actually occurs within the EU or EEA; or
- A controller or processor not established in the EU/EEA that controls or processes personal data of data subjects *located* in the EU/EEA if processing occurs in connection with (a) offering goods or services to the data subject even if no payment is required, or (b) monitoring the data subjects' behavior within the EU/EEA; or
- "[P]rocessing of personal data by a controller not established in the [EU] but in a place where Member State law applies" pursuant to "public international law."

Fines

- May be imposed on an "undertaking," which may consist of several corporate entities
- Fines for non-compliance can be up to the greater of 2 percent of annual global sales or €10M.
  - Children's personal data (Art. 8)
  - Processing not requiring identification (Art. 11)
  - Data protection by design and default, controller/processor obligations, record keeping, cooperation with supervising authority, security of processing, breach notification, data protection impact assessment (Art. 25-39)
  - Certification (Art. 42)

Fines (Cont'd)

- Fines for non-compliance can be up to the greater of 4 percent of annual global sales or €20M.
  - Principles relating to processing of personal data (Art. 5)
  - Lawfulness of processing (Art. 6)
  - Consent (Art. 7)
  - Processing special categories of personal data (Art. 9)
  - Data subjects' rights (Art. 12-22)
  - Transfers of personal data to third country to international organization (Art. 44-49)
  - Obligations under Member State law
  - Non-compliance with Supervisory Authority limitation/ suspension or failure to provide access

Other Penalties

- Criminal sanctions
- Reprimand in lieu of a fine
- Further remedies or corrective orders in addition to a fine

GDPR Considerations

- Consent
- Breach notification
- Technical and organizational processes to respond to data subjects' exercise of rights
  - Right to be Informed
  - Right to Access
  - Right to Rectification
  - Right to Erasure
  - Right to Portability
  - Right to Restrict Processing
  - Right to Object to Processing
  - Right Not to be Subject to Automated Decision Making

GDPR Considerations (Cont'd)

- Technical and organizational processes to fulfill obligation to comply with data protection by design
- Technical and organizational processes to fulfill obligation to ensure appropriate security measures
- Maintain records of processing activities
- Data protection impact assessment for new technologies
- Transfers of data to third countries or international organizations

QUIZ: Does the GDPR Apply?

Crazy Rich Company has offices in the United States exclusively. They sell power tools to companies located in Lichtenstein, which is not a member of the EU.

Yes ☐ No ☐

Astrid Leong is vacationing in NYC from Paris. She sends emails to Charlie Wu, who is in Paris.

Yes ☐ No ☐

Peik Lin runs a business out of her California apartment, selling rap CDs to anyone who wants to buy one through her website, which tracks only what visitors place in their shopping cart.

Yes ☐ No ☐

Princess Intan, a Malaysian citizen, makes purchases on Chanel.com while in Amsterdam.

Yes ☐ No ☐

Prof. Rachel Chu, a professor located in America, emails with professors at Oxford University in the UK.

Yes ☐ No ☐

Mahjong.com is a company with a single office in Atlanta, Georgia. It does not sell products nor market outside of the United States. Its website is visited by individuals located all over the world. Website visitors cannot provide any information through the website.

Yes ☐ No ☐

Young Enterprises, located in Madrid, Italy, sells chocolate all over the world. It does not use a computer system but, instead, keeps paper records.

Yes ☐ No ☐

Practical Example #1 – "Personal Data"

- Business relevance – all users
  - The protective services team supports an executive during a visit to Libya. While on the visit, the executive's location is tracked and this location information stored in Control Risks' systems.
  - The forensic accounting team interviews the team members of a client's finance team in connection with a suspected fraud. The Chief Finance Officer says that he suspects the Finance Manager has stolen account information from their systems.
  - One of Control Risks' external IT suppliers employs five temps in their call center to deal with an increase in call volumes. In accordance with the IT services agreement, it sends Control Risks the names and work email addresses of the temps.

How does each scenario relate to personal data?

Practical Example #2 – "Controller" or "Processor"?

- Business relevance – all users, especially CFI, Legal Tech and data analysis
  - A client asks Control Risks to carry out a due diligence task, during which it collects various personal information about a director of a company the client wishes to acquire.
    - ***Controller or processor?***
  - A client asks Control Risks to image a hard drive on one of its employee's laptops and to analyze the data it finds.
    - ***Controller or processor?***
  - A client asks Control Risks to host two terabytes of data for its lawyers to pore over as part of a regulatory investigation.
    - ***Controller or processor?***

Practical Example #3 – "Lawful Basis"

- Business relevance – all users
  - The crisis response team intercepts and records a phone call between members of a group of kidnappers holding a government official, in which a number of the kidnappers are named.
  - The business intelligence team gathers information on individuals in a local, anti-government trading network for a client looking to set up a nearby trade route.

Which lawful basis does Control Risks rely upon in each scenario?

Practical Example #4 – "Fair Processing Notices"

- Business relevance – online solutions, marketing
  - Control Risks' marketing team adds a 'sign-up' button to its website, where users can register to receive a newsletter, product information and promotional offers. Registrants will also be added to a database to receive invites to industry events.
  - A member of the event security team works with the PA of a VIP guest attending a trade submit, including gathering information about the medication she takes and her immediate family. This information is sent securely to everybody in the security team.

Would a fair processing notice need to be given?

GDPR Impact and Developments Since May 25, 2018

What Does This Mean for You?

Evolution of Data Privacy Generally and in the United States

- 1973 – Data Act
- 1974 – Privacy Act of 1974
- 1988 – United Nations, Office of the High Commissioner for Human Rights Art. 17
- 1995 – Data Protection Directive
- 2000 – Safe Harbor
- 2016 – Privacy Shield

Data Protection/Privacy Officers (DPOs) and Chief Compliance Officers (CCOs)

- Federal Trade Commission (FTC)
- Department of Justice (DOJ), Securities and Exchange Commission (SEC) and Registrants
- DPO and CCO similarities

Similarity between U.S. and EU Law

- Bill of Rights – does not address
- Patchwork of U.S. laws, including, but not limited to:
  - Financial Services Modernization Act (GLBA)
  - Fair Credit Reporting Act (FRCA)
  - Fair Debt Collection Practices Act (FDCPA)
  - Children's Online Privacy Act (COPPA)
  - Health Insurance Portability Act (HIPAA)

Potential Conflict of Laws between U.S. and EU Regulations

- Financial Crimes Enforcement Network (FinCEN) Customer Due Diligence Rule
- USA Patriot Act
- Federal Rules of Civil Procedure
- Hague Evidence Convention
- Local and Federal Privacy Laws (*e.g.*, HIPAA)

Comments by the U.S. Government

- Commodity Futures Trading Commission (CFTC)
- Department of Homeland Security (DHS)

Third-Party Resources

- EDRM at Duke Law
- The Sedona Conference

GDPR Enforcement and Developments Since May 25, 2018

Phillips Lytle LLP

Thank You