International Implications of Privacy Rights:
US - Microsoft Ireland case & CLOUD Act
EU - GDPR and Schrems II

DeBrae Kennedy-Mayo
Georgia Tech Research Faculty Member
Attorney-at-Law
March 23, 2018
US Reputation on Privacy

- US has no privacy protections
  - Incomplete and actually not accurate
- By the end of the presentation, my goal will be to have you understand a different narrative
My Background

- Research Faculty Member at Georgia Tech’s Scheller College of Business
  - Research legal and policy issues related to cybersecurity and privacy
- Team
  - Peter Swire – formerly in White House on these issues
  - Jack Leahey – in Audience
- Co-teach Business Law class to undergraduates
My Background

- Attorney for 15 years
  - Worked as Assistant Attorney General for State of Georgia for 8 years
    - Represented Governor, Secretary of State, State Ethics Commission, State Elections Board, Judicial Branch, and Board of Regents
  - Worked in private practice for several years
- Worked as an Assistant District Attorney in both metro Atlanta (Clayton County) and Savannah
  - Live in Savannah, Work in Atlanta
My Background

- Publications
  - 2002 - “In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty [Budapest Convention]”
    - Article included in Book entitled *Computer Crime* (Ashgate Publishing)
  - “Crawford v. Washington: A Retro Protection Guaranteeing the Right to Confrontation?”
    - South Carolina Bar Journal
Co-Authorered Publications

- **U.S. Private Sector Privacy: Law and Practice for Information Privacy Professionals**
  - Book, International Association of Privacy Professionals (forthcoming next week)
  - “Why Both the EU and US are ‘Stricter’ than Each Other for the Privacy of Government Requests for Information”
      - Will discuss in this talk
Places I have traveled internationally

- Siberia – Russia
- Hong Kong – China
- Australia
- Europe
Privacy as travel internationally

- Lot of ways to think of privacy
  - “Right to be Left Alone”
  - Think of privacy = control
- Control over data
  - Who can collect
  - Who can use
  - Who can disseminate
US: Privacy Expectation - Encryption

- **Apple v. FBI (2016)**
  - San Bernardino shooting
  - Law enforcement wanted access to phone
    - Phone encrypted
  - Law enforcement wanted Apple to create a back door to get into encrypted phone
  - Apple said if broke encryption for this one instance then would break it for everyone
  - Ultimately, not settled by court
  - FBI found another way to get info
  - So far, encryption protected in US
Russia and Privacy Protections

“Telegram Loses Bid to Block Russia From Encryption Keys”

Bloomberg – March 20, 2018

Telegram, the encrypted messaging app that’s prized by those seeking privacy, lost a bid before Russia’s Supreme Court to block security services from getting access to users’ data, giving President Vladimir Putin a victory in his effort to keep tabs on electronic communications.

Putin signed laws in 2016 on fighting terrorism, which included a requirement for messaging services to provide the authorities with means to decrypt user correspondence.
Ripped from the Headlines

- China and Privacy Protections
  - “Apple Moves iCloud Data and Encryption Keys for Chinese Users to China”
    - *The Hacker News* – February 28, 2018
      - “This is the first time when Apple is going to store encryption keys required to unlock iCloud accounts of its users outside the US.”
      - “In theory, Chinese law enforcement agencies won't have to ask US courts for compelling Apple to give them access to the Chinese users’ data.”
Australia and Privacy Protections

“Australian Government Tries to End Encryption Once Again”

The Merkle – January 27, 2018


As part of the proposal, Australian government agencies would be able to collect communications data in bulk.

This pertains to both internet and phone-based communication throughout all of Australia.
The new law restores or extends previous emergency provisions, such as empowering police to carry out raids and local authorities to place suspects under house arrest without prior judicial approval.

It also expands those powers, for example allowing the police to search luggage and vehicles without judicial warrants.

In addition it reinstates warrantless seizures of computer and cellphone data that France’s highest legal authority had struck down as unconstitutional, adding a few restrictions that still fall short of judicial oversight.
US: Strong Privacy Related to Gov’t Access

- **US Constitution**
  - 4\(^{\text{th}}\) Amendment – Search warrant requirement for law enforcement (government) to access data (papers)
    - Based on “probable cause” that a crime has occurred
      - Ex. Clayton County – phone (unencrypted)
  - 5\(^{\text{th}}\) Amendment – Right against self-incrimination
  - 6\(^{\text{th}}\) Amendment – Right to counsel in a criminal case
    - “Miranda Rights”
    - “Exclusionary Rule”

- **Statute - Electronic Communications Privacy Act (ECPA)**
  - Request to US service providers for electronic evidence.
    - Interpreted to say - Law enforcement needs to obtain warrant based on probable cause to get content of stored data.
US privacy developments this year

- **Microsoft Ireland Case**
  - US DOJ served search warrant on Microsoft for all documents it held on person (third-party request)
  - Microsoft gave all documents it held on US soil
  - For all documents held by Microsoft in Ireland, company told government to request through Ireland system.
  - Microsoft did this even though it could access the documents electronically at its home office in the US.
    - Documents stored by Microsoft on servers located in Ireland.
    - Federal court ruled that Microsoft was correct, as warrant did not have extraterritoriality reach.
  - Case before US Supreme Court

- **Cloud at issue**
  - Cloud – Great Marketing: Means Remote Servers
US privacy developments this year

- CLOUD Act - Expected to pass today in Omnibus Act
  - Legislation currently before the Congress that would solve the issue in the *Microsoft Ireland* case
  - Legislation would allow other countries to make direct request of US service providers AND
  - US law enforcement to make direct request for data held in other countries
US privacy developments this year

- **CLOUD Act**
  - Addresses problem that most requests for information are related to local crimes
    - Ex. French burglary with French victim and French perpetrator
    - Evidence has been emails, social media, and other electronic communication related to crime
    - US service provider holds data, and US service provider located on US soil
  - Will make it easier for these law enforcement officers in other countries to get electronic evidence
    - Average delay on these requests to US has been 10 months to get electronic evidence
US privacy developments this year

- **CLOUD Act**
  - Legislation would authorize a series of bilateral agreements (agreements between 2 nations) – Ex. US-UK
  - Each country would agree to a set of privacy protections for the data
  - **NOTE:** These agreements would not require “probable cause” for law enforcement to access data in the US
    - US is basically only country in the world that requires this standard
    - Even EU has not been willing to give data this level of protection in a criminal proceeding
    - NOT raise the bar to US standard
    - Hope to raise at least somewhat in many places
From US to EU: Privacy Protections

- US: Privacy Protections against Gov’t
  - *Microsoft Ireland* case
  - CLOUD Act
- EU: Privacy Protections against Companies
  - GDPR
  - *Schrems II*
EU: Privacy Protections Against Companies

- GDPR: General Data Protection Regulation
  - Becomes Effective May 25, 2018
  - Protects the data of Europeans within EU and as it travels outside the EU
  - Fines can be as high as 4% of a company’s global revenues
    - Ex. Delta (online stat): $41 billion in revenue
    - 4% of $41 billion = $1.6 billion
GDPR: A Primer

- Individual Rights of Data Subjects (Individuals)
  - Right to Access
  - Right to Rectification
  - Right to Be Erasure ("To Be Forgotten")
    - US: analogy in credit after 7 years
    - EU: much broader
  - Right to Restrict Processing
  - Right to Data Portability
  - Rights in Relation to Automated Decision Making and Profiling (Data Analytics, Big Data, Etc.)
EU: Requirements for Data to Leave EU

- Must be a lawful basis for transfer of EU data to another country (even fly out on a plane)
  - Country level
    - Country must have been determined to be ‘adequate’ in its privacy protections
  - OR
  - Company level
    - Must have another lawful basis – Companies make promises in how they will handle data
      - Agreement between US-EU
        - Safe Harbor (now struck down)
        - Privacy Shield
      - Standard Contract Clauses
      - Binding Corporate Rules
EU: Countries deemed to be ‘adequate’

- Traditionally have looked at whether country has comprehensive privacy laws – protecting person against intrusion by business
  - Comprehensive – applies to all electronic data (regardless of type)
    - From mental health records to phone number
    - If comprehensive, likely found to be adequate
  - If do not, then adequacy decision goes against country
    - US has sectorial privacy laws
      - HIPPA – Medical Privacy
      - COPPA – Children’s Privacy Online
      - FTC – Unfair and Deceptive Practices by Business
EU: Countries deemed to be ‘adequate’

- Andorra
- Argentina
- Canada (commercial organizations)
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
EU: Requirements for Data to Leave EU

- Must be a lawful basis for transfer of EU data to another country (even fly out on a plane)
  - Country level
    - Country must have been determined to be ‘adequate’ in its privacy protections
  - OR
  - Company level
    - Must have another lawful basis – Companies make promises in how they will handle data
      - Agreement between US-EU
        - Safe Harbor (now struck down)
        - Privacy Shield
      - Standard Contract Clauses
      - Binding Corporate Rules
EU: Privacy protections against companies

- Schrems I case (2015) – Case against Facebook
  - Europe’s highest court, the European Court of Justice, struck down the EU/US Safe Harbor Agreement as a legal basis for transferring data between the EU and the US
    - Facebook not protecting data when it goes to US
  - Why?
    - In large part, concern over NSA’s foreign intelligence surveillance practices – Snowden disclosures (2013)
      - *NOT much the company can do about this
Technology and Legal Protections

- Signals Intelligence (electronic communication) collected from Service Providers (on US soil)
  - **PRISM Program** – Government collects to/from information from a “targeted selector” (email – such as terrorist1234@isis.net) directly from the Service Provider
    - NSA then applies minimization procedures

- Signals Intelligence (electronic communication) collected from Backbone of the Internet (on US soil)
  - **Upstream program** – All traffic from the Backbone is collected, targeting procedures and minimization procedures are electronically applied, and then a person in government reviews the data
    - *Think about this for a minute*
    - International implications – discussed later
EU: Privacy Protections Against Companies

- **Schrems I case - 2015**
  - The European Court of Justice struck down the EU/US Safe Harbor Agreement as a legal basis for transferring data between the EU and the US
  - **Why?**
    - Concern over NSA collection practices – PRISM and Upstream
    - Concern over how US persons treated “better” than others for collection of foreign intelligence

- **Schrems II case - 2018**
  - Current Case concerns whether Standard Contract Clauses will continue to be a lawful basis for transfer of personal data from the EU to the US
  - Max Schrems questioned whether there are adequate safeguards against surveillance by the US government for data transferred to the US
  - **Why is there a concern that this case will come out against US?**
    - US still has NSA’s PRISM and Upstream in place
EU: Requirements for Data to Leave EU

- Must be a lawful basis for transfer of EU data to another country (even fly out on a plane)
  - Country level
    - Country must have been determined to be ‘adequate’ in its privacy protections
  - OR
  - Company level
    - Must have another lawful basis – Companies make promises in how they will handle data
      - Agreement between US-EU
        - Safe Harbor (now struck down)
        - Privacy Shield
      - Standard Contract Clauses
      - Binding Corporate Rules
EU: From Concern over Company Practices to Concern over Foreign Intelligence Surveillance Practices in US

- EU is concerned about foreign intelligence gathering practices of US
  - NSA and PRISM and Upstream programs
- EU: ?
  - Begs the question about practices by countries in EU
EU: From Company to Surveillance

- EU: Do not do analysis of European countries surveillance by agencies like their NSA because part of EU
  - Can’t do look under EU Treaty – Lisbon Treaty
  - National security left to European countries because national security issue where EU has no jurisdiction
  - Presumed under the Lisbon Treaty (agreement to make EU) that European countries’ practices are ok
EU: From Company to Surveillance

- EU: Do not do analysis of European countries surveillance by agencies like their NSA because part of EU
  - Presumed under the Lisbon Treaty (agreement to make EU) that European countries’ practices are ok
  - National security left to European countries because national security issue where EU has no jurisdiction

- UK: This legal fiction will cease once Brexit occurs
  - UK will have to undergo adequacy determination once not part of EU
    - Will look at MI-6 practices (their FBI)
EU: From Company to Surveillance

- Independent Assessment of Systemic Privacy Protections from Government Assessment
  - Oxford University Study
    - US: “Benchmark” for the World for Transparency and Oversight – Systemic Privacy Protections
    - Foreign Intelligence Surveillance Act (FISA)
    - Foreign Intelligence Surveillance FISC – Federal judge with life-time tenure reviews foreign intelligence surveillance practices, and has power to stop actions of NSA
  - Congressional Oversight
    - Review Group & Privacy and Civil Liberties Oversight Board (PCLOB)
- EU Countries: Did not compare as well as US
  - UK, Germany, France
EU: From Company to Surveillance

- US: Reforms after Snowden
  - Peter Swire: Member of Presidential Commission that made 47 recommendations
  - 70% put into place
  - People in US can advocate for change when do not like aspects of their government
US: Adequacy Decision – Plus Factors

- Schrems II case
  - In our research and writing at Georgia Tech, we have emphasized “plus factors” in US system
    - May not have Comprehensive Approach to Privacy Against Companies
    - Look at US system overall
US: Adequacy Decision – Plus Factors

US
- Sectorial Approach +
- Plus Factors
  - Democratic Government with Checks and Balances
  - Independent Judiciary
  - Constitutional Protections of Individual Rights
  - Democratic Accountability
  - Transparency and Oversight for Foreign Intelligence Surveillance Programs – such as PRISM and Upstream
  - “Benchmark”

EU
- Comprehensive Approach
China: Adequacy Decision – Minus Factors

**EU**
- Comprehensive Approach

**China**
- Comprehensive Approach (arguably on the books – may or may not actually do)
- Minus Factors
  - Social Credit System
  - Video Surveillance
  - Voiceprint Database
  - DNA Database
  - Great Firewall of China
### US Reputation on Privacy – More Accurate Narrative

<table>
<thead>
<tr>
<th>Protections against business intrusion</th>
<th>Protections against government intrusion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>US – Sector Approach</strong></td>
<td><strong>US</strong></td>
</tr>
<tr>
<td>- Federal - FTC, FCC, CFPB, SEC</td>
<td>- Constitution</td>
</tr>
<tr>
<td>- State – Office of State Attorneys General</td>
<td>- ECPA</td>
</tr>
<tr>
<td>- EU – Comprehensive Approach</td>
<td>- FISA (foreign intel)</td>
</tr>
<tr>
<td>- GDPR</td>
<td>- EU</td>
</tr>
<tr>
<td></td>
<td>- Not as strict as US</td>
</tr>
<tr>
<td></td>
<td>- Advocate for lessening of protection provided by ECPA</td>
</tr>
</tbody>
</table>
US Reputation on Privacy – More Accurate Narrative

Protections against business intrusion

- **US – Sector Approach**
  - Enforcement has been in the multi-millions of dollars

- **EU – Comprehensive Approach**
  - Will begin to give out large fines

Protections against government intrusion

- **US**
  - Constitution
  - ECPA
  - FISA (foreign intel)

- **EU**
  - Not as strict as US
  - Advocate for lessening of protection provided by ECPA
US Reputation on Privacy – More Accurate Narrative

- Make your own determinations about what is sufficient to protect privacy in the US, in the EU, and in other places around the world.
- Do so with a more complete narrative of the protections that currently exist.
Research at Georgia Tech

- Cross-Border Requests for Data Project
  - Institute for Information Security and Privacy (IISP) - http://www.iisp.gatech.edu/cross-border-data-project

- Schrems Testimony

- Current Paper
  - Why Nationality Matters When Discussing Foreign Intelligence
Upcoming Conference

- Institute for Information Security & Privacy (IISP)
  - Georgia Tech Cybersecurity Summit (2018)
  - Save the Date: October 4, 2018
  - Topic: Nation-State Attacks
  - [https://cyber.gatech.edu/2017-cyber-security-summit](https://cyber.gatech.edu/2017-cyber-security-summit)
Questions

- Professor DeBrae Kennedy-Mayo
- debrae.kennedy-mayo@scheller.gatech.edu