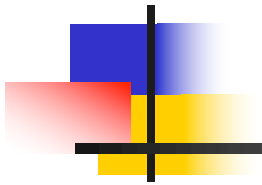


Beyond the Basics: Recent Developments in Global Data Privacy and Security

David Bender
Special Counsel, Data Privacy
GTC Law Group
Distinguished Fellow, Ponemon Institute

The Universe of Current Privacy Concerns

- The Privacy world is today confronted with two broad critical problems, and innumerable narrower, but nevertheless important, specific problems.
- The two broad critical problems: Establishing and maintaining an appropriate degree of Privacy while:
  - (1) permitting the cross-border transfer of personal data, especially from the EU, & most especially from EU to US; and
  - (2) funding the ever-increasing informational benefits generated by the worldwide web.

But First, a Word About EU Privacy Law – The Times, They are a-Changin'

- The EU recently enacted a "General Data Protection Regulation" ("GDPR") with a framework similar to that of the "Data Protection Directive," which is the basis for current EU law.
- The GDPR will replace the Directive on **May 25, 2018**.
- The GDPR embodies many significant changes from the Directive.

Two GDPR Provisions Will Make EU Privacy Law More Important to Many, Many US Companies

- Jurisdiction: GOTCHA! – GDPR purports to apply to any entity – whether or not it has a presence in the EU -- that processes the personal data of EU residents in connection with offering goods or services to, or monitoring the behavior of, persons in the EU.
- Sanctions: OUCH! Maximum penalty for GDPR violation -- set with Google & Facebook in mind -- is the greater of €20 million, or 4% of annual worldwide revenue.

The 1st Critical Problem: Crisis in the Export of Personal Data from the EU

- Both the EU's existing law (the Directive), and its forthcoming law (the GDPR), have provisions restricting cross-border transfer ("XBT").
  - The two sets of restrictions are similar.
- Why are the XBT restrictions so important?
  - Because if US importers can't find a viable vehicle for export, they cannot legally acquire or use personal data transferred from the EU.

Cross-Border Transfer ("XBT")

- Under both the Directive and GDPR, for lawful transfer, you need one of these bases:
  - "adequacy" of transferee law;
  - contractual safeguards;
  - consent; or
  - one of several "necessities."
- The US has been deemed not to have "adequate" data protection laws.

Safe Harbor

- In 2000, US and EU negotiated a "Safe Harbor":
  - Export was permitted to US importers agreeing to the "Safe Harbor Principles"
- Functioned reasonably well for 15 years.
- In October 2015, the EU's highest court (European Court of Justice – "ECJ") ruled that the EU decision approving Safe Harbor was invalid, thus striking down the program.
  - One main basis: US national security surveillance was viewed as violating EU residents' fundamental rights.

The Aftermath

- Companies had to find some "safe" means of export.
- US-EU negotiated "Privacy Shield," the successor to Safe Harbor, which debuted on August 1, 2016.
- But there is an inherent problem:
  - ECJ did not just find a flaw in the Safe Harbor mechanism for exporting the data;
  - rather, it also found fault as to data treatment in the US.
- That perceived deficiency will seemingly exist no matter what means are used to export the data.
- Privacy Shield is already the subject of litigation seeking to invalidate it, as are "standard contractual clauses," another popular export vehicle.

EU Misconceptions about US National Security Surveillance

- The Snowden revelations sparked outrage in the EU.
- June 5, 2013 news report: the content of all EU e-mails flowed directly to NSA.
- On June 6, the same journalists in the same newspapers corrected that statement: only the content of e-mails that recited certain identifiers (*e.g.*, names or e-mail addresses of suspects) was sent to NSA.
- The truth never caught up with the misstatement.

The US, the EU, and National Security Surveillance

- Three extensive studies have compared the surveillance laws of numerous nations, including the US and many EU Member States.
- Findings: few if any nations incorporate more restrictions on collection, use, and disclosure, or more protections for individuals, than the US.
- No evidence of US intel community's intentional or widespread failure to follow requirements of US law.

Latest Cross-Border Transfer Development: Irish Court Sends SCC Matter to the ECJ

- On Oct. 3, 2017, an Irish court referred to the ECJ the matter of the validity of standard contractual clauses ("SCCs") for transfer of personal data to the US.
- SCCs are probably the most frequently used vehicle for export from the EU.
- The Irish opinion echoed concepts espoused in the ECJ decision that struck down Safe Harbor.

The Bottom Line on Cross-Border Transfer

- As a result of EU paranoia regarding US surveillance, & the ECJ's refusal to balance Privacy against other interests as required by EU law, the ECJ may end up invalidating ***every*** practical data export mechanism.
- Coupled with the draconian penalties permitted under the GDPR, this poses an export crisis that should catch the attention of every entity in the US that relies on personal data from the EU.

Critical Problem #2: Funding the WWW

- Today, in the WWW, we have at our fingertips a treasure trove of information, mostly without paying money directly for access.
- This "free" access to information is supported by a complex arrangement among various players in the online advertising industry.
- Advertising pays to support this structure (and these costs are passed on to consumers).

Slicing and Dicing

- This structure works because, through complex and proprietary analytics, the industry is able to determine (by IP address) which users likely have an interest in a particular product/service, and to sell appropriately addressed ads, often in real time.
- As a result:
  - Online advertisers can send far fewer ads;
  - Consumers get far fewer ads that don't interest them; and
  - To support this, consumers must supply an enormous amount of personal information about all phases of their lives.

Killing the Goose?

- The OBA industry argues that consumers willingly trade information for free content.
  - Advertising revenues paid to websites fund free content.
  - Absent massive data collection, WWW users will have to pay for content, resulting in a vastly changed landscape unacceptable to users.
- The missing element: a robust, detailed, public discussion on:
  - (i) the details of how restricting the collection of user data may reduce website funding; and
  - (ii) feasible alternatives for funding websites.

Effect of GDPR on Online Behavioral Advertising (OBA)

- Jurisdictional: GDPR applies to the processing of personal data, of persons in the EU by an entity not established in the EU, that relates to monitoring the behavior of individuals in the EU.
- Substantive: With exceptions, an individual has a right not to be subject to a decision based solely on automated processing that produces legal effects about, or similarly significantly affects, him or her.

Who Owns the Internet?
The Right to be Forgotten

- EU Data Protection Directive: When processing of an individual's personal data fails to comply with the Directive, the individual has a right to erasure of the results. GDPR also includes a right to be forgotten.
- 2014 ECJ [EU's highest court] case involved Google name search on a man who, twelve years earlier, was mentioned in news articles announcing an auction connected with an attachment proceeding to recover certain debts.

The Right-to-be-Forgotten

- 2014 ECJ [EU's highest court] case involved Google name search on a man who, twelve years earlier, was mentioned in news articles announcing an auction connected with an attachment proceeding to recover certain debts.

The case began in 2009 when Mario Costeja, a lawyer in Spain, objected that entering his name in Google's search engine led to legal notices that he said were no longer relevant. Cabalar/European Pressphoto Agency

Right to be Forgotten (continued)

- Directive: The interests of data controllers (like search engine operators) and third parties (like users) must be balanced against a person's fundamental privacy rights.
- Held: The individual prevailed.
  - Here, the information was stale and largely irrelevant.
  - Google must take down links to the articles.
  - Different result if individual were a public figure.

Subsidiary Right to be Forgotten Issue

- What may Google say when it deletes a link?
- In results of name searches, Google states links may have been omitted to comply with EU law.

Some results may have been removed under data protection law in Europe. Learn more

- Google also informs the website in question, identifying the web page.
- The EU asserts that Google must not disclose this information.
- This matter has not yet been resolved.

The Major Remaining RTBF Issue

- Issue: To which Google websites does the injunction against linking apply?
- EU position: All Google websites worldwide.
- Google position: Only those websites with EU domains (*e.g.*, .fr, .de, .uk).
- Present Status: Google was fined €100,000.
  - In July 2017 this matter was referred to the ECJ for a ruling.

New York State Dep't of Financial Services Cybersecurity Rule -- Guidelines for All?

- NYS DFS issued an extensive Cybersecurity Rule, effective March 1, 2017.
- Applies directly only to financial services providers that require a license from, or are chartered by, NYS.
  - But will influence many large multinational institutions that seek uniformity worldwide.
  - Contains much that is valuable for enhancing the security of companies across the board.
  - One of the best cybersecurity roadmaps around.

Warrants for Electronic Records

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
SEARCH WARRANT

TO: CHIEF OF POLICE OR ANY OTHER LAW ENFORCEMENT OFFICER
(Specific law Enforcement Officer or Classification of Officer of the Metropolitan Police Department or other Authorized Agency)

AFFIDAVIT, herewith attached, having been made before me by Detective Greggory Pemberton (D2-1645) that he has probable cause to believe that in the premises controlled by DreamHost Inc., there is now being concealed property, namely stored electronic communications including but not limited to digital files, records, messages, and photographs as set forth more fully in Attachments A and B, attached hereto and incorporated herein.

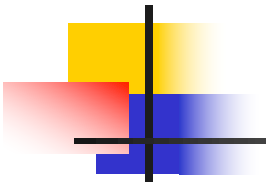
WHICH IS in violation of D.C. Code § 22-1322 and as I am satisfied that there is probable cause to believe that the property so described is being concealed in the above designated electronic storage and remote computing service and that the foregoing grounds for issuance of the warrant exist,

YOU ARE HEREBY AUTHORIZED, within **10** days of the date of issuance of this warrant, to execute this warrant by emailing or faxing this warrant to the designated electronic storage and remote computing service for execution of a search of its electronic files for the electronic data specified, and if the electronic data be found there,

DreamHost, IS ORDERED TO ASSIST LAW ENFORCEMENT AND PRODUCE SUCH ELECTRONIC DATA, as detailed in Attachments A and B, to Detective Greggory Pemberton, and AUSA John Borchert

Warrants: Is Data Stored Abroad Fair Game?

- In civil litigation, Rule 34 Requests for Production and Rule 45 subpoenas require a person to search for and produce documents (including electronic documents) in its possession, custody, or control.
  - Subject to the usual objections, they are typically enforced if the recipient is present in the US, no matter where the information and documents are.
- In criminal matters, warrants generally permit the government to enter and conduct the search itself.



The Stored Communications Act

- But in 1986, Congress enacted the Stored Communications Act ("SCA").
- The SCA permits federal and state courts to issue warrants on probable cause requiring communications service providers to produce the content of communications stored in their systems.
- SCA warrants are served like subpoenas on communications service providers (*e.g.*, telcos and Internet service providers), who are then required to search and produce the described content.

Extra-territorial Warrants (continued)

- Issue: Can an SCA warrant served in the US on a company present in the US require it to produce data in its possession or control that is located outside the US?
- *Microsoft* – SCA warrant served on Microsoft in US demands production of data, about a suspect, stored in a Microsoft server in Ireland.
- *Google* – SCA warrant served on Google in US demands production of data, about a suspect, stored in Google server(s) located outside US, but Google does not know in what country(ies).

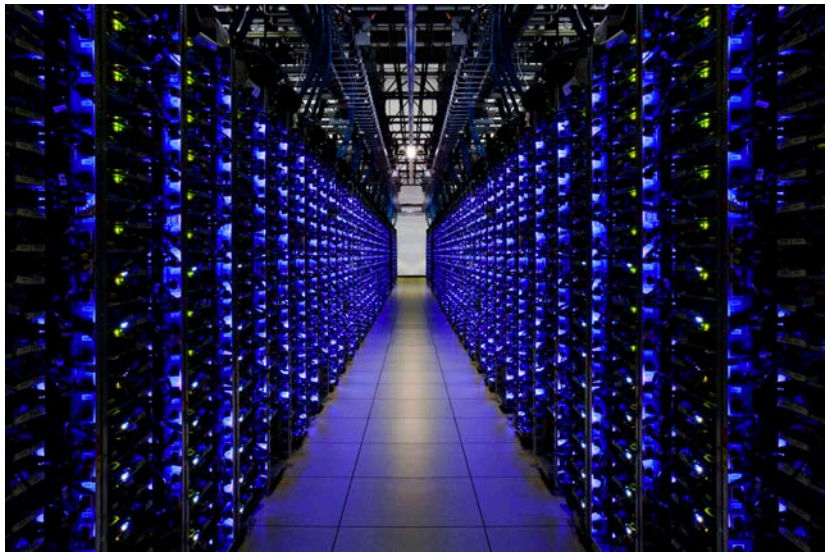
Microsoft Data Center in Dublin, Ireland

2013 Construction

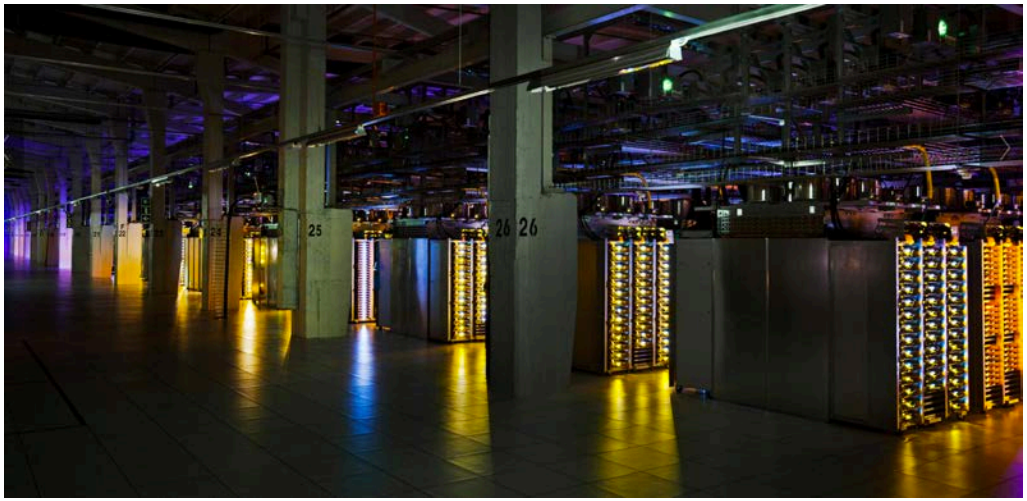
Extra-territorial Application (Microsoft)

- *Microsoft* (2nd Circuit 2016) – Federal legislation is presumed to apply only in US unless contrary intent clearly appears.
  - No contrary intent appears in SCA.
- Term "warrant" is used in 4th Amendment, to restrict government searches and seizures in domestic matters.
- Court saw the conduct that falls within focus of SCA as taking place outside US.
- Although MS would act only in US, data was in Ireland and MS would have to interact with its Irish data center.
- Court was not persuaded by fact that, as practical matter, there was no other way for government to get the data.
- Held: Warrant was unenforceable.

Google data centers in US and EU



Georgia, US



Finland

Google

- Magistrate judge (E.D. Pa. 2017) (and several similar cases) - The crimes occurred solely in US.
- Google system has servers in many countries, but data can be retrieved only from a terminal in US.
- Google produced only the data stored in the US, relying on *Microsoft*.
- Google's system automatically transfers data from one server to another (and one country to another) to optimize performance.
  - Google can't determine where a particular file is stored.

Google (continued)

- Magistrate judge read *Microsoft* as focusing on user privacy and concluding that enforcement would be extraterritorial because Microsoft – the government's agent - would seize the data in Ireland.
- Google court:
  - There would be no seizure, as there would be no interference with the account holder's possessory interest.
  - Search would take place in US, as that is where Google would interfere with suspect's expectation of privacy by retrieving data and turning it over to government.
- Enforcement does not involve extra-territorial application.

Google (continued)

- This would merely be a permissible domestic application of the SCA.
- Even if a foreign state's sovereignty would be implicated, it is impossible to ID that foreign state.
- And because of the manner in which Google stores data, the government would not be able to use the MLAT process.
- Thus, unless the SCA warrant were enforced, there is no practical way for the government to get the data.
- The government's motion to compel was granted.

Privacy Can Interfere with other Important Values

- National security,
- Law enforcement,
- Freedom of speech,
- Public health,
- Medical care,
- Avoidance of fraud,
- Candor,
- Right to engage in business,
- Right to access information,
- Transparency, and
- ***Even the right to live.***

Example of Privacy Interference with National Security: Suspect in Berlin Terror Attack Dec. 2016

- German police quickly identified a suspect.
- In an attempt to apprehend him, his name and picture were widely publicized across Europe.
- But because of restrictive German privacy laws, German media used only his first name and last initial, and a modified photo of him.

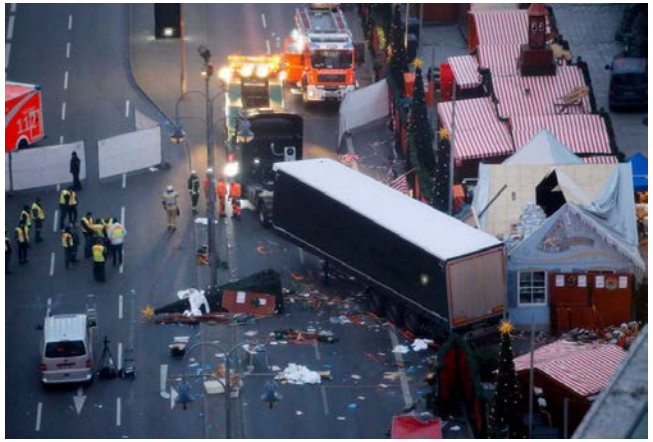


Photo Used by German Media in the "Attempt" to Apprehend Suspected Terrorist

Compare to more typical US reporting

David Bender, Esq. **1996**

Example of Privacy Interference with the Right to Live: Andreas Lubitz

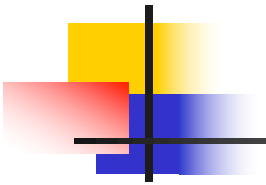
- Pilot for airline Germanwings.
- Suffered from severe emotional distress for years.
- Succession of therapists all diagnosed severe depression.
- Some told him he should not be flying.
- None informed the government or his airline.
  - German medical privacy law prohibited disclosure.
- On March 27, 2015, Lubitz intentionally flew his Airbus, with 149 other persons aboard, into a French mountain.

Why Should This Matter to You?

- A US analysis of what is a "legitimate business use" or a "necessity" for cross-border transfer or processing may be very different from an EU analysis.
- If a DPA deems it neither necessary nor legitimate to use a full-face image of a suspected terrorist, will that DPA think it proper to use EU resident data for profit-seeking business purposes, such as marketing?

Suggestion for the Day

- In the near term, the single best investment a company can make in Privacy is to enhance its data security.
- Reason: The regulators will be fully occupied with privacy violations that are foisted on them – they will have little time to go looking for additional violations.
  - So the object is to make sure you are not one of the companies that come to the attention of regulators.
- If this all sounds depressing, keep in mind the story about the two hikers and the bear.



QUESTIONS?