2017: Privacy Issues on the Horizon

January 19, 2017
Today’s Presenters

Liisa M. Thomas
Chair, Privacy and Data Security Practice
Chicago, London
lmthomas@winston.com

Robert H. Newman
Partner, Privacy and Data Security Practice
Chicago
rnewman@winston.com
Overview

• Data Breach
• The European Privacy Landscape
• The “Internet of Things”
• Privacy and Security in China
• Industry-Specific Privacy Requirements
• Mobile Tracking
Data Breach
Audience Question One

As a consumer, do you feel protected by breach notice laws?
New U.S. State Laws That Took Effect in 2016

- Oregon
- Nebraska
- California
- Tennessee
- Rhode Island
GDPR: Beginning May 2018

72 hours
What’s Next?

??

© 2017 Winston & Strawn LLP
Audience Question One: Results
Audience Question Two

As a consumer, when (not if) you get a notice that your personal information has been breached, do you feel harmed?
Spokeo: Why Aren’t There Fewer Cases?

• Spokeo, Inc. v. Robins (May 2016)

• Court held that statutory violations, alone, aren’t enough to satisfy the injury requirement for Article III standing
  • Because the harm to the plaintiff from a defendant’s mere statutory violation is not “concrete”

• However, a “concrete” harm need not necessarily be “tangible”

What is a concrete harm is thus unclear
No Harm

- *Kamal v. J. Crew Grp., Inc.* (U.S. District Court for the District of New Jersey)
  - J. Crew printed more than five credit card digits on in-store sales receipts, in potential violation of FACTA
  - Court held that the supposed harm of the FACTA violation (a heightened risk of potential future identity theft) is not concrete
Harm

- *Flaum v. Doctor’s Associates Inc.* (U.S. District Court for the Southern District of Florida)
  - Subway operator printed five debit card digits plus an expiration date on in-store sales receipts, in potential violation of FACTA

- *Carlos Guarisma v. Microsoft Corp* (U.S. District Court for the Southern District of Florida)
  - Microsoft retail store printed first six digits of credit card, plus last four, on plaintiff’s printed sales receipt, in potential violation of FACTA

- Courts reasoned that FACTA confers a substantive right (rather than a procedural right)
  - In *Guarisma*, court held “Where Congress has endowed plaintiffs with a substantive legal right, as opposed to creating a procedural requirement, the plaintiffs may sue to enforce such a right without establishing additional harm”
How Courts Will Rule…

Right now not easy to predict, cases thus likely to continue…
Audience Question Two: Results
The European Privacy Landscape
GDPR Will Usher in New EU Privacy Regime

• **May 2018:** General Data Protection Regulation (GDPR) will repeal and replace the EU Data Privacy Directive

<table>
<thead>
<tr>
<th>Key Changes from Data Protection Directive</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU-wide regulation (not country-by-country)</td>
</tr>
</tbody>
</table>

© 2017 Winston & Strawn LLP
Audience Question(s) Three

Will your company be adding a Data Protection Officer (DPO) to address GDPR?

If not, is it because you already have a DPO?

If not, is it because you don’t have EU operations?
Do You Need a Data Protection Officer Under GDPR?

Companies with core activities that require regular and systematic monitoring of individuals on a large scale. Article 37(1)(b). But what does that mean in practice?
Core Activities

Those that are key to achieving a company’s goals (e.g., processing of patient data by a hospital)
Regular and systematic

Ongoing or recurring on a fixed basis in a manner that shows some planning or strategy

- Online profiling
- Online tracking
- Retargeting
- Location tracking
- Loyalty program
- Monitoring fitness (wearable)
Large scale

Standards likely to develop over time…

Processing customer geo-location data for statistical purposes related to the company’s services

Processing customer data in “regular course of business”
Audience Question(s) Three: Results
Privacy Shield: Will it Gain Traction?

Will EC re-evaluate effectiveness annually?

How burdensome will vendor management be for enforcing contractual provisions?

How will the new U.S. administration impact certainty and predictability?

Will Department of Commerce really give greater scrutiny than under Safe Harbor?

But even if not … it can help to go through the process and get your “privacy house in order”
Reminder: Alternatives to Privacy Shield

Model Clauses

Binding Corporate Rules
The “Internet of Things”
Do you have a connected device (a wearable fitness monitor, baby monitor, home security camera, Internet-connected fridge, Internet-connected thermostat)?
What is the Risk?

October 2016: Massive DDoS attack of Dyn web servers using connected “smart” consumer devices with default usernames and passwords
Regulators Taking Notice

FTC settlement with ASUSTeK
- A cloud computing and router company
- FTC alleged that gaps in ASUSTeK’s products’ security violated its promises to protect consumer information (i.e., a deceptive act)

15 state AGs settle with Adobe for $1 million
- Data breach impacted more than half a million users
- AGs were concerned by Adobe’s alleged lack of mechanisms to detect and respond to unauthorized activity in its systems
Audience Question Four: Results
Privacy and Security in China
Audience Question Five

Does your organization have operations in China or work with third parties (like suppliers) from China?
Draft Regulations to Update Consumer Rights Protection Law

• Reiterates existing data privacy rules under the 2013 Consumer Rights Protection Law
  • E.g., disclosure and consent requirements, data security measures

• New requirements
  • Data collection must be relevant to the business operations
  • No electronic marketing or telemarketing without consent
  • “Personal information” expanded to include biometric data

• New exception: Operators may transfer data without consent if it has been desensitized so an individual cannot be identified
New Cybersecurity Law Raises Concerns for Non-Chinese Organizations

• Broad new powers for Chinese government to investigate crime and protect IT systems

• Permits the Chinese government to audit organizations and require security certification
  • Potential effect: Chinese government could obtain proprietary information (e.g., source code) and encryption keys for sensitive systems

• Also requires companies to store data locally
  • Potential impact on cross-border data transfers
    • Data processors must obtain government permission before transferring consumer or other important information out of the country

• Will take effect June 2017
Audience Question Five: Results
Industry-Specific Privacy Requirements
Audience Question Six

Do you feel like you have a strong handle on existing legal requirements about how your organization can collect, use, and store information, including how your organization can interact with consumers using their information?
Everyone “Wants In” on the Privacy Game

- Requirements on organizations continue to proliferate
- Critical to understand what information a company holds, how it gets it, how it is used, and how it is protected
Audience Question Six: Results
FCC’s Recently Finalized Privacy Regulations

• Applies to Internet service providers (ISPs)
• New rules for collecting “sensitive data”
  • Defined to include children’s information, health and financial information, geolocation records, and Internet browsing history
• ISPs must get express prior consent (i.e., opt-in consent) from customers before collecting “sensitive” data
FCC Regs vs. Other Regulatory Oversight

• FCC (opt-in) vs. FTC (opt-out) for collecting
• If FCC preempts state law, yet another layer of complication

Confusion

FCC
FTC
State AGs

© 2017 Winston & Strawn LLP
CFPB Begins Privacy Enforcement Efforts (Financial Services)

First enforcement against Dwolla (online payment platform)

- Settlement over alleged misrepresentations over data security claims
- Claimed to be “safe” and “secure”
- Per CFPB: Dwolla allegedly failed to encrypt sensitive data, conduct risk assessments, or train employees

$100,000 civil penalty

Draft / implement data security plan

Annual audits to identify security flaws

Employee training

2x per year internal security assessments

Board responsible for implementing and overseeing compliance

Appoint someone to lead data security program

Draft / implement data security plan
Mobile Tracking
Audience Question Seven

Do you play *Pokémon GO*?
Pokémon GO and Geolocation Tracking Disclosures
Audience Question Seven: Results
FTC’s Take on Geolocation

- FTC recs: “Mobile Privacy Disclosures: Building Trust Through Transparency”

  - Just-in-time disclosures
  - Affirmative consent

- InMobi settlement (June 2016)
  - Mobile advertising network allegedly bypassed location settings on users’ phones to collect location data

- Must get EXPRESS consent for location tracking
- Must delete improperly obtained location data
- Nearly $1 million civil penalty
- Annual audits for 20 years

© 2017 Winston & Strawn LLP
Industry Self-Regulation on Geolocation

• Digital Advertising Alliance mobile privacy guidelines on precise location data and third-parties
  - Provide **notice** of third-party collection or sharing ("clear, meaningful, and prominent")
  - Get **consent** for third-party collection or sharing

• DAA Accountability Program enforcement against iTriage
  - Mobile app allegedly failed to disclose collection/sharing of location data with third parties for interest-based advertising
  - Settlement terms
    - Ceased collecting and sharing precise location data with third parties
    - Added just-in-time notifications for data collection in app
Want More Information?

• Winston Privacy Year In Review 2016
  • http://cdn2.winston.com/images/content/1/1/v2/118486/Privacy-YIR-DEC2016.pdf
Thank You.

Liisa M. Thomas
Chair, Privacy and Data Security Practice
Chicago, London
lmthomas@winston.com

Robert H. Newman
Partner, Privacy and Data Security Practice
Chicago
rnewman@winston.com