HOW TO NAVIGATE THE LANDSCAPE OF GLOBAL PRIVACY AND DATA PROTECTION

Paul Jones, Jones & Co.

Kathleen Rice, Faegre Baker Daniels, LLP
Topics to Cover

- General Concepts
  - Increased U.S. enforcement activity
  - U.S. vs. International
  - Impact on franchises

- Data Breaches
  - Costs, sanctions and liability

- Recent Developments
  - United States:
    - *FTC v. Wyndham; LabMD; Spokeo*
    - Legislation and industry standards
  - International:
    - GDPR; Privacy Shield

- What It All Means for Franchises
  - Identifying and mitigating risks
  - Privacy policies and practices
  - Insurance
Introduction

• Previously much concern about proper notices and forms of consent

• Enforcement was not common in Europe or the U.S.

• Now the main issue is security – and breaches

• And now even fast food is paid for with a wave of a credit card

• Enforcement is becoming more common
General Concepts:
Increased Enforcement Activity
International

• U.S. privacy law is the outlier – most countries have general privacy laws

• Stronger enforcement over last decade

• Data localization – driven by concerns over U.S. security efforts

• GDPR and Privacy Shield
General Concepts:
Increased Enforcement Activity

• Domestic

• Federal Trade Commission
  • Lead Federal enforcer
  • Section 5(a) of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. Sec. 45(a)(1).
  • “Unfair” practices = “cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C. Sec. 45(n).

• State Enforcement
  • State Attorneys’ General
    • State statutes on data protection and privacy; Unfair and deceptive acts
General Concepts: U.S. vs. International

- U.S. —Regulated sectors; becoming less of a model for other countries
  - Internationally the U.S. is now an outlier
- EU—General privacy law: GDPR—in effect May 2018
- Canada—PIPEDA/provincial laws
- Singapore – changed its mind – now has a privacy law
- China—No general privacy law yet, but under discussion
General Concepts: Impact on Franchises

• Data protection and risk of data breaches are key concerns

• Need to consider international implications, not just domestic
  • Comply with general data protection laws, rather than just sector-specific laws

• Who’s responsible for data security/privacy and compliance?
  • Franchisor or Franchisee? – The Wyndham case

• Design privacy and security system that can comply with general laws, not just sector-specific or U.S. law
Data Breaches

• In General: Unauthorized acquisition, access, use, or disclosure of personal information
• Usually exemption for encrypted or redacted data
• Increasing costs, including notification, credit monitoring, and investigation
• Sanctions/Fines may be significant; may be more than just monetary
• Liability
  • Regulatory enforcement
  • Common law claims
  • Class actions
Data Breaches Can Result in:

• Litigation issues, especially state claims/potential class actions
• Regulatory investigations and enforcement
• Negative publicity/reputation
• Financial loss
• Loss of clientele
• Loss of productivity
• Damage to employee morale
• Loss of consumer confidence
• Additional costs
Recent Developments: United States

• Litigation/Regulatory Enforcement
• Legislation
• Industry Standards
FTC v. Wyndham, 3rd Circuit, August 2015

• Overview:
  • Hackers accessed Wyndham Worldwide computer systems on three occasions in 2008 and 2009
  • 619,000 consumers affected
  • Over $10.6 million in fraudulent charges
  • FTC alleged Wyndham’s conduct in responding to/preventing incidents was unfair and privacy policy was deceptive
  • Wyndham challenged FTC’s authority to regulate cybersecurity under the unfairness prong of section 5 of the FTC Act.
FTC v. Wyndham

- FTC’s complaint alleged that Wyndham engaged in unfair cybersecurity practices that unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.

  - e.g., Storing payment card info in clear readable text; allowing use of easily guessed passwords to access property management systems; failing to use readily available security measures, such as firewalls.

- District Court granted Wyndham motion to dismiss. FTC appealed.
**FTC v. Wyndham, December 2015 Settlement**

- Wyndham must:
  - Establish comprehensive information security program to protect cardholder data—including payment card numbers, names, and expiration dates.
  - Conduct annual information security audits and maintain safeguards in connections to its franchisees’ servers.
  - Obtain annual security audits of its information security program that conform to the Payment Card Industry Data Security Standard for certification of a company’s security program.
FTC v. Wyndham, December 2015 Settlement

• Wyndham’s audit must certify:

  • The “untrusted” status of franchisee networks, to prevent future hackers from using the same method used in the company’s prior breaches;

  • The extent of compliance with a formal risk assessment process that will analyze the possible data security risks faced by the company; and

  • That the auditor is qualified, independent and free from conflicts of interest.
FTC v. Wyndham, December 2015 Settlement

• If Wyndham suffers another data breach affecting more than 10,000 payment card numbers, they must obtain an assessment of the breach and provide that assessment to the FTC within 10 days.

• Wyndham’s obligations under the settlement = 20 years.
FTC Enforcement: LabMD

• FTC alleged that LabMD’s data security practices were inadequate following alleged breach

• Administrative Law Judge sided with LabMD and found that FTC had failed to prove that LabMD’s security practices caused or were likely to cause substantial injury

• FTC overruled ALJ and concluded the disclosure of health information causes harms that may not be economic or physical in nature but are real and substantial under section 5

• LabMD has appealed to Eleventh Circuit Court of Appeals
Data Breach Consumer Class Actions

• Sound primarily in tort (negligence), but plaintiffs also sue for breach of contract, breach of fiduciary duty, invasion of privacy under state law, consumer fraud, unfair competition, violation of state data breach laws, violation of Fair Credit Reporting Act, etc.

• Plaintiffs seek recovery of damages arising out of:
  • Cost of fraud
  • Risk of future identity theft
  • Burden of fixing things—e.g., closing affected accounts
Consumer Class Actions

• Have not met with much success

• Standing: Is “increased risk” theory sufficient?

• Damages: Even if “increased risk” theory passes standing bar, can it establish damages element of tort claim?

• Causation: How do you show, for example, that fraudulent charge resulted from a particular breach?
Other Security Breach Litigation

- By credit card companies, banks, and other issuing entities
- Based on negligence
- Damage allegations arise out of issuing new cards, reimbursing fraudulent transactions
Standing to Sue: 
Spokeo, Inc. v. Robins, U.S. Supreme Court, 13-1339

• Issue
  • May Congress give an otherwise uninjured plaintiff Article III standing to sue by passing a law and granting a private right of action to the plaintiff to sue for its violation?

• Holding
  • No, and Yes
Spokeo

• *Article III* requires a “concrete” injury, meaning a *de facto* one

• To be “concrete,” an injury can be either tangible or intangible

• The risk of injury can be sufficient
**Spokeo**

- Congress cannot grant standing in the absence of a concrete injury
  - But Congress can elevate risks that were previously legally inadequate into injuries that are adequate
- “Bare procedural violations” of statutes do not create standing
  - Credit reporting agency listing an incorrect zip code
  - Failure to give notice of use of accurate information
Recent Developments: United States

• Legislation:
  • State legislative efforts continue, with respect to breach notification requirements and heightened security measures
  • Federal data breach legislation still under consideration: Yahoo breach

• Industry Standards:
  • New PCI-DSS
  • Continued efforts to develop best practices by federal agencies, working groups, companies

Recent Developments: International

• **US-EU Privacy Shield**
  - Affects transfers of personal data into the U.S. for commercial purposes
  - Includes:
    - Redress mechanisms for individuals
    - Privacy policies with right to access and disclosure of data
    - Accountability for onward transfers of personal data
    - Additional safeguards and notice with respect to third-party data transfers
  - Safe Harbor-compliant companies will likely not have difficulty certifying
  - More than 700 self-certified by October 1
  - Uncertain legal future; Binding Corporate Rules and Model Clauses still options

• **General Data Protection Regulation**
Background to the GDPR

• Regulation replaces the 1995 Data Protection Directive and the national laws pertaining to the Directive
• Much greater level of harmonization than at present
• One law, directly applicable in all 28 Member States
• Will apply beginning May 25, 2018
• European data privacy standards are going global
• International privacy policies will need to be GDPR compliant
• 99 Articles, 173 Recitals, 3,999 amendments
• The most heavily lobbied piece of European legislation ever
The potential costs of non-compliance

• Potential for significant fines:
  • DPAs can impose fines of up to €20m or 4 percent of worldwide turnover for some infringements, such as improper processing of data

• Private right of action (Art.78-79)
  • If data subject is not satisfied with the DPA's response to his or her complaint, then may bring a complaint before a national court
  • Right of collective representation by not-for-profit bodies – class actions
  • Some European firms are already developing plaintiff litigation plans
Putting It Into Perspective

• Regulators will take into account:
  • the nature, gravity and duration of the infringement
  • whether infringement was intentional
  • categories of personal data affected
  • steps to mitigate the damage suffered
  • degree of responsibility (e.g. data protection by design or by default) or any relevant previous infringements
  • adherence to a code of conduct (or certification mechanism)
  • cooperation with the supervisory authority (and the manner in which supervisory authority learned of infringement)
  • compliance with measures ordered
  • other aggravating or mitigating factors (e.g. financial benefits, etc.)
The Biggest Issue—Territorial Scope

• Data Protection Directive
  • companies established in the EU; or
  • companies which make use of equipment (automated or otherwise) situated in the territory of a EU Member State

• GDPR
  • EU data protection law applies to data controllers or processors based outside of the EU which:
    • offer goods or services to EU data subjects (whether for payment or for free); or
    • monitor the behavior of EU data subjects (regarding activities of the data subjects within the EU)
Offering Goods or Services (In a Little More Detail)

• Not caught by:
  • mere accessibility of a website, e-mail address or other contact details
  • mere use of language in the controller’s country (e.g., English or Spanish)
  • will not apply to geo-blocked sites

• However, more likely to be caught if, e.g.,
  • there are sales in local currencies e.g., € or £
  • the possibility of ordering goods or services in that language
Why U.S. Franchises Should Be Concerned

• Significant extra-territorial reach of GDPR

• GDPR and Privacy Shield may require changes to:
  • privacy policies
  • internal procedures
  • technology platforms
  • vendor/third-party agreements

• Significant penalties for non-compliance under GDPR, private right of action

• Compliance with data privacy laws will be on a similar level with antitrust or anti-bribery and corruption
What It All Means for Franchises

• Identifying and mitigating risks

• Privacy policies and practices

• Insurance
Identifying and Mitigating Risks

• Ongoing risk assessments and privacy audits
  • Identify personal information collected and used
  • Identify characteristics of data, including source, age of subject, where it is stored, encrypted/redacted, retention period
  • Identify third-party access and contractual obligations

• Monitor legal and regulatory environment, internationally and in U.S.
• Learn from enforcement actions, including security practices
• Periodically, and after incident, re-assess policies, practices, and risk
Identifying and Mitigating Risks

• What can we learn from Wyndham?

  • If you do not assess the risks posed by your franchisee operations, then, as in Wyndham, you have not assessed all the risks

  • Previously some franchisors were content just to require franchisees to “comply with local privacy laws”

  • Now may wish to consider providing the franchisees with a template privacy policy and monitoring their compliance
Privacy Policies and Practices

Appoint a Privacy Officer?

• In Canada this is mandatory

• Will soon be mandatory in Europe for some companies under the GDPR

• In any event because of the size of the risks, senior executive buy-in is key
Privacy Policies and Practices

• Companies violate the deceptiveness prong of FTC Act when they make inaccurate statements about their privacy practices.

• Privacy policies must be accurate:
  - Say what you mean, mean what you say
  - Assume FTC will interpret privacy policy very literally
Privacy Policies and Practices

• Make them readable, understandable to ordinary person—avoid extensive legalese

• Ensure they capture elements required by international, federal, and state law, e.g., CA
Privacy Policies and Practices

• If your franchise system is international, or has plans – consider using an international standard

• In Canada, it is mandatory for all businesses to have a privacy policy and to make it available

• Business are limited to collecting only the personal information reasonably required for the purposes – this is usually how to tell a U.S. privacy policy from a Canadian privacy policy
Privacy Policies and Practices

10 PRINCIPLES

1. **Accountability** – privacy officer, responsibility for outsourced information

2. **Identifying Purposes** – personal information will be used for marketing, payment, performing service, etc.
Privacy Policies and Practices

10 PRINCIPLES

3. Consent – the knowledge and consent of the individual are required for the collection, use and disclosure – with certain key exceptions

4. Limiting Collection – collection is limited to what is necessary for the purpose identified
Privacy Policies and Practices

10 PRINCIPLES

5. Limiting Use, Disclosure and Retention – personal information can be used or disclosed only for the purpose for which it was collected

6. Accuracy – personal information shall be up-dated regularly
Privacy Policies and Practices

10 PRINCIPLES

7. Safeguards – personal information shall be protected by security safeguards appropriate to the sensitivity of the information

8. Openness – privacy policies shall be readily available to the public
9. **Individual Access** – Individuals may request information about their personal information that is held by the business. They also can have access, and they can challenge the accuracy of the business records.

10. **Challenging Compliance** – there has to be a complaint system internal to the business
Insurance

• About 50 insurers offer cyber risk coverage in the U.S. today
• Huge increase in interest in the last 5 years.
• Who is buying?
  • Early purchasers = technology, financial, healthcare
  • Last few years = retail, manufacturing, professional services
  • Today = adding more small and mid-sized businesses
• Not standard coverage—products vary with little case law interpretation. Experienced insureds/brokers need to read and understand differences
Insurance

• Typically can cover:
  • Liability for security or data breaches
  • Costs associated with data breach (e.g. notification costs, credit monitoring)
  • Costs associated with restoring, updating, or replacing electronically stored business assets
  • Business interruption and extra expense from a security breach and contingent business interruption (e.g., suppliers’ or customers’ cyber loss causes you business interruption)
  • Cyber extortion or cyber terrorism expenses
  • Business website, social media or print media liability associated with libel, slander, copyright infringement, and product disparagement

• What’s not covered: Costs from cyber espionage
Insurance

• Some Pitfalls:
  • Thinking your standard commercial general liability policy covers data breach damages
    • Most cover only direct physical loss to property of another, not data
    • Most include data breach exclusion
  • Not allocating enough time to purchase:
    • Cumbersome application process takes time
    • Management, not just IT questions, involved
  • Not budgeting for this cost separately in insurance budget
Insurance

  • Contractual Obligations to the Bank
    • $1.7 million in fraudulent charges
    • $200,000 in notification, card replacement costs and administrative fees.
  
  • had a “CyberSecurity by Chubb Policy”
    • so-called “Privacy Injury” coverage actually only applied to the person whose data was illegally accessed, and not the retailer
    • exclusion was for contractual liabilities that the retailer had assumed
Summary

• Can you still afford to delegate privacy compliance to your franchisees?

• Security issues generate more issues than having the perfect consent form

• What works in the U.S. is unlikely to work in the rest of the World
Questions?

Paul Jones, Principal  
+1 416-703-5716  
pjones@jonesco-law.ca

Kathleen Rice, Counsel  
+1 574-239-1958  
kathleen.rice@FaegreBD.com