IDI International Distribution Institute

Protection and exploitation of data in distribution networks

Who is the “owner” of the customers’ data?

IDI International Distribution Institute

Who is the “owner” of the customers’ data?

Speakers

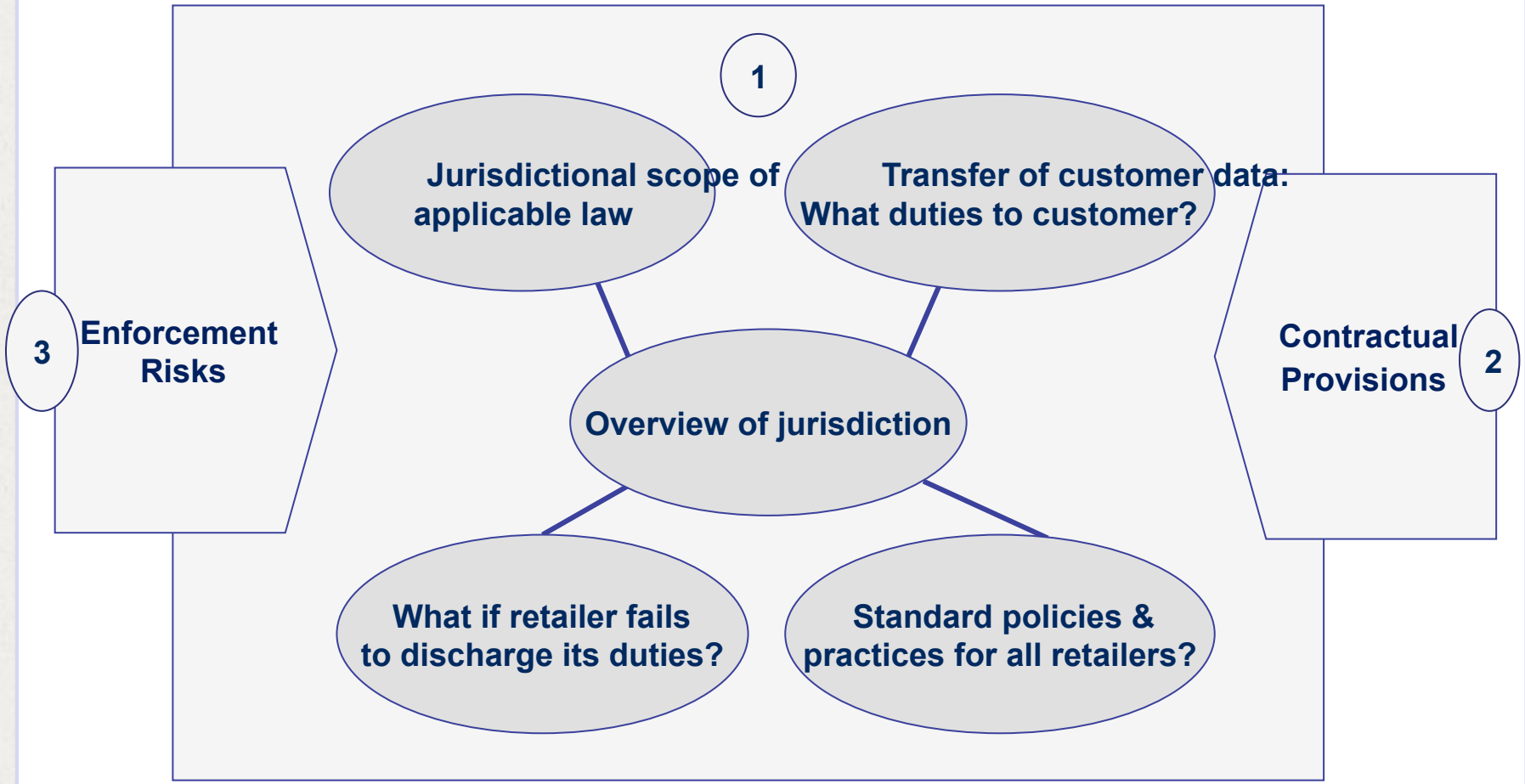
Paul Jones
Jones & Co.
Toronto, Canada

Giorgia Armanni
FURLA S.p.A.
Bologna, Italy

Michael K. Lindsey
Steinbrecher & Span
Los Angeles, California

IDI International Distribution Institute

Meeting Agenda and Framework of Reference



1. Brief Overview of Each Jurisdiction's Privacy Protections for the End User Customer Whose Data is Gathered by Retailer

1. If customer data will be forwarded from retailer to manufacturer / franchisor, what are each party's duties to customer?
2. What if retailer fails to discharge its duties?
3. Should manufacturer / franchisor prescribe standard policies and practices for all retailers?

International Distribution Institute

1. Overview of Each Jurisdiction's Privacy Protections for the End User Customer Whose Data is Gathered by Retailer

GDPR
May 25 2018

YESTERDAY

Several Interpretation of the same EU directive 95/46/CE on data protection

2018

One single law for all EU member countries

Local law for certain detail aspects

1. Overview of Each Jurisdiction's Privacy Protections for the End User Customer Whose Data is Gathered by Retailer – Legal Framework

- **European Directive on Privacy (95/46/CE)**
- **Italian data protection code (Legislative Decree)**
- **Italian Data Protection Authority measures and guide lines www.garanteprivacy.it**
- **Opinion of Art. 29 Working Party**
- **New General Data Protection Regulation 679/2016 (effective as from May 25, 2018)**

1. Overview of Each Jurisdiction's Privacy Protections for the End User Customer Whose Data is Gathered by Retailer – Legal Framework- PRC

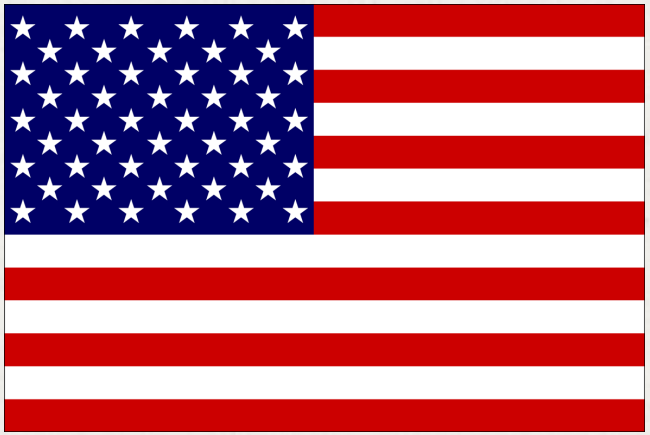
- **The PRC was developing a European style privacy law, but events intervened in 2010 with a dispute between internet giants Tencent and Qihoo**

- **Result is broad principles in the new 民法总则 (General Principles of the Civil Law or Book One of the future Civil Code) adopted in 2017 and in the 侵权责任法 (Tort Liability Law – 2010) and a variety of sector specific laws, regulations and guidelines**

- **More recently under the 网络安全法 (Cybersecurity Law – 2017) there are specific privacy standards**

1. Overview of Each Jurisdiction's Privacy Protections for the End User Customer Whose Data is Gathered by Retailer – Legal Framework

- No centralized, comprehensive national privacy law
- Sectoral approach:
  - Financial
  - Health
  - Homeland Security
- FTC – Primary federal authority: FTC Act §5
  - "unfair" prong
  - "deceptive" prong
- Individual states
  - Many have "little FTC Acts"
  - Several large "resolution payments" recovered in privacy and data security cases
  - All 50 have data security breach notification laws



1. Overview of Each Jurisdiction's Privacy Protections for the End User Customer Whose Data is Gathered by Retailer – Legal Framework - Canada

- **For international matters and for internal matters in most provinces – *Personal Information Protection and Electronic Documents Act* – (PIPEDA)**

- **Federal Court says federal Privacy Commissioner has the power to protect information of Canadians internationally**

- **Québec, British Columbia and Alberta have provincial laws**

- **Sector specific health laws in several provinces**

- **Supreme Court case re doctor's records says that doctor owns the paper files, but patient owns the data – patient received complete access**

International Distribution Institute

If Customer Data Will be Forwarded From Retailer to Manufacturer/Franchisor, What are Each Party's Duties to Customer?

Franchisor = Data Controller

The controller is responsible for and must be able to demonstrate compliance with these principles

Data transfer outside EU only subject to appropriate measures

It shall comply with principles of lawful processing

Purpose limitation

It shall comply with rights of

Data minimisation

Integrity and confidentiality

Storage limitation

Accuracy

International Distribution Institute

If Customer Data Will be Forwarded from Retailer to Manufacturer/Franchisor, What are Each Party's Duties to Customer?

Franchisee = Data Processor

The Processor process personal data on behalf of the controller. Processor shall be GDPR compliant.

- **Implement and comply with an adequate contractual framework (DPA) with Controller**
- **Being available to auditing**
- **Restrict the appointment of sub data processor**
- **Keep records on processing activity**
- **Implement adequate security**
- **Answers to requests made by data subject and inform the data controller**
- **Cooperate with supervisory authority and data controller**
- **Keep data inside EU, where required**

If Customer Data Will be Forwarded from Retailer to Manufacturer/Franchisor, What are Each Party's Duties to Customer? - PRC

- **Under the Cybersecurity Law the 信息安全技术 个人信息安全规范 (Information Security Technology Personal Information Security Specification) was released in January 2018**

- **It is only a guideline, and cannot be used for enforcement directly. However compliance with it would be generally considered compliance with the general principles stated in other laws**

- **Previously privacy issues had not arisen in PRC franchise and distribution deals – but this year a prospective franchisee refused to request customer permission for the transfer of customer data to the U.S.**

If Customer Data Will be Forwarded from Retailer to Manufacturer/Franchisor, What are Each Party's Duties to Customer?

- In general, depends on terms of retailer's privacy policy
- Required disclosures
  - Again, a sectoral approach
    - Financial sector requirement
  - States have taken lead
    - Mandatory disclosures
      - Transfers to affiliates
      - Transfers for marketing purposes
- Broad no-transfer policy statements may trigger enforcement action if policy not observed
- What if privacy policy fails to address manufacturer/franchisor transfers?

If Customer Data Will be Forwarded from Retailer to Manufacturer/Franchisor, What are Each Party's Duties to Customer? - Canada

- **Under PIPEDA each retailer or franchisee is required to have a privacy officer, a privacy policy and to be responsible for personal information transferred to third parties for processing**

- **For a transfer to franchisor to be lawful, notice must be given, the purpose must be reasonable, and the consent of the individual must be obtained**

- **When transferring data internationally, the practice is that the destination country should be specified**

- **The recipient of data under these provisions must be bound by contract to provide a comparable level of privacy protection**

IDI International Distribution Institute

Potential Protections for Retailer Compiling the End User Customer's Data

- Intellectual property
  - Retailer may claim trade secret protection for list of its customers
  - Whoever gathers, collects, assembles or maintains data may own copyright
    - Work made for hire doctrine likely does not apply to retailer
    - Possibility of contractual assignment
- Unfair competition / related law
  - Retailer may have privacy law duties to customers
    - In such cases, and in absence of contract provisions, would it be unfair competition for manufacturer/franchisor to require access to customer data?

2. Contractual Provisions

- Range of manufacturer / franchisor approaches to protecting customer data
  - Laissez faire approach
    - Potential for brand damage
  - Required compliance with applicable laws or policies
    - Potential for inconsistent interpretations
    - Enforcement of sharing requirement
  - Providing training and standard templates
    - Policing, enforcement and alter ego issues

2. Contractual Provisions

- In the absence of optimal protections (e.g., a legacy contract), what other provisions may be applicable?
  - Compliance with laws requirement
  - Operating manual compliance
  - Trademark / branding approval of
    - Use of trademark
    - Advertising
  - Operational standards approvals
  - New technology or systems requirements
  - Management approval requirement

Impact of Expiration or Termination of Contract between Retailer and Manufacturer/Franchisor

- Does manufacturer/franchisor have right to transfer or purchase of certain of retailer's assets?
  - If not, does retailer have continued right to use data?
  - What does privacy policy(ies) say about continued use?
  - What does privacy policy(ies) say about transfer to manufacturer / franchisor?
  - What does applicable law provide?

3. Enforcement Risks

- Governmental agency enforcement
- Private actions
- Class actions
- The role the issue of damages plays in impacting enforcement

IDI International Distribution Institute

What if Retailer Fails to Discharge its Duties as Data Processor?

Failure to comply with GDPR and Data Processing Agreement

- **The supervisory authority will investigate the compliance practices and highlight any areas that fail to meet the GDPR's requirements**
- **The GDPR gives supervisory authorities the power to issue fines of up to €20 million or 4% of the breached organisation's annual global turnover, whichever is greater for certain infringement and up to €10 million or 2% of the company's global annual turnover, for other infringements**
- **The supervisory authority will investigate the compliance practices and highlight any areas that fail to meet the GDPR's requirements**
- **Member States have the ability to apply penalties for infringements to the GDPR. The Member State will be responsible for implementing such penalties, which must be effective, proportionate and dissuasive (Italy has provided for imprisonment)**
- **Individuals have the right to claim compensation for any damage suffered as a result of violating the GDPR**

3. Enforcement risks

- Governmental agency enforcement
  - *FTC v. Wyndham Worldwide*
  - *LabMD, Inc. v. FTC*
- Private actions – key issues
  - Standing
  - Damages
  - Insurance
- Class actions
  - Typicality requirement
- The role of damages issue in impacting enforcement

3. Enforcement risks - Canada

- Governmental agency enforcement
  - Privacy Commissioner's orders are not binding
  - But Commissioner can apply to court to make them binding, some awards of damages for humiliation
- Private actions under provincial privacy tort laws and common law tort of "intrusion upon seclusion"
  - *Douez v Facebook* – privacy rights are strong cause to over ride a choice of law and forum
  - Damages – *Jones v Tsige* - upper limit of $20,000 absent monetary loss, punitive damages may be available
- Class actions – several ongoing

3. Enforcement risks - PRC

- Governmental agency enforcement
  - Art. 64 of the Cybersecurity Law allows the competent department to require corrective action, confiscate illegal income, levy a fine based on such income or otherwise
  - In serious cases the department may suspend the operations of the infringer
- Private actions would be under the Tort Liability Law
  - An NGO protecting consumers sued the search engine Baidu in January 2018 – case was settled when Baidu agreed to correct its behavior – example of representative action
- Private Action under the Anti-Unfair Competition Law
  - In 2016 an internet social media company collected user's personal information off its competitor Weibo's web site – damages of 2 million RMB

IDI International Distribution Institute

Case Study

IDI International Distribution Institute

Who is the “owner” of the customers’ data?

Questions / Discussion

Paul Jones
Jones & Co.
Toronto, Canada

Giorgia Armanni
FURLA S.p.A.
Bologna, Italy

Michael K. Lindsey
Steinbrecher & Span
Los Angeles, California