Data Protection, Data Privacy, and Duty of Care
The U.S. Perspective

Ron N. Dreben, CIPP
Morgan, Lewis & Bockius LLP

Let’s talk about the “patchwork”

- Financial information
  - Gramm-Leach-Bliley Act and the “Safeguards Rule”
  - Credit card information and PCI-DSS compliance
- Medical information
  - Health Information Portability and Accountability Act of 1996 (HIPAA)
  - Personal Health Information (PHI) must be protected in compliance with the HIPAA Privacy Rule
- Children’s information
  - Children’s Online Privacy Protection Act (COPPA)
- Student Information
  - Family Education Rights and Privacy Act (FERPA)
- Commercial Email, Email Scanning and Email Hacking
- Video Privacy Protection Act
- Text messaging, Cell Phone Calls and Faxing

50 States and Privacy Laws

- Medical and financial information
- Personally Identifiable Information in General
- Biometric data, including facial recognition
- Social security numbers
- Drivers licenses
- Mug shots
- Age
- Obligations to encrypt
- Obligations to have privacy policies and to comply with them
- Obligations to report and respond to data breaches

Privacy Shield

- As of mid-October, more than 1500 companies, including Google, Microsoft and DropBox, have submitted self-certifications under the Privacy Shield framework.
- The United States has given the European Union assurances that the access of public authorities for law enforcement and national security purposes is subject to clear limitations, safeguards, and oversight mechanisms.
- The US has stated it will not perform indiscriminate mass surveillance of personal data transferred to the US under the Privacy Shield arrangement.
- The US Secretary of State has established possible redress for EU residents through an “ombudsman” mechanism within the US Department of State.

Examples of Data Collection by Businesses

- Spokeo
- The Vibrator Case
- Talking Barbie
- Pokemon Go
- Information collected by your car
- Information collected by hotels
- Contests and Sweepstakes
- Yahoo breach
- Personal Data and Bankruptcies
- Drones

Making Consumers More Comfortable with Disclosing Data

- Privacy Policies
- Opt-in's, Privacy Controls and Access/Control of Personal Information
- Privacy Certifications (Data Privacy Management companies)
- Bug bounty programs, or vulnerability disclosure programs
- "White hat" hackers test security
- PCI-DSS credit card controls
- Tokenization – a non-sensitive unique identifier instead of the original data
- Watchdog associations like EPIC (Electronic Privacy Information Center) and Electronic Freedom Foundation (EFF)
- Credit watching services

U.S. Government Guidance and Enforcement

- Federal Trade Commission (FTC) actions based on security breaches and improper or unfair personal data collection.
- FTC released a January 2015 report identifying its information security expectations for companies that manufacture health monitors, home security devices and other “internet of things”.
- The FCC more recently approved new rules for Internet Service Provider’s use and sharing of customer data.
- US Food and Drug Administration (FDA) provided privacy guidance in January 2015.
- Office of the Comptroller of the Currency (OCC) has issued guidelines regarding cyberattacks.
- The U.S. Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) has taken enforcement actions against investment advisers and broker dealers for failing to take reasonable steps to protect customer records and information.
- National Infrastructure Protection Plan of 2013.

U.S. Government Data Collection

- Electronic Communications Privacy Act of 1986
- The U.S. Patriot Act and Foreign Intelligence Surveillance Act (2008 amendments)
- Edward Snowden
- Private companies (for example, Apple, Microsoft and others) challenging government requests for personal data and “gag” orders

About Ron N. Dreben

Ron N. Dreben

Partner

Washington DC

T +1.202.739.5213

ron.dreben@morganlewis.com

Ron N. Dreben advises clients on intellectual property and technology issues in business transactions. He provides advice in connection with mergers, acquisitions, and licensing arrangements, as well as trademark, copyright, trade secret, and related IP law. A Certified Information Privacy Professional (CIPP), Ron helps companies address privacy issues and respond to security breaches and advises US companies on the relevance of the EU Data Directive. Ron has experience negotiating with most of the leading technology product and service vendors.

Ron counsels clients on all aspects of IP issues as they merge or acquire businesses. He conducts worldwide IP diligence, and addresses IP representations and indemnification, and confidentiality and noncompete provisions.

Ron handles IP documentation in a host of other types of transactions. He drafts and reviews IP, technology, and software agreements. Additionally, Ron has experience creating website hosting and e-commerce agreements, terms and conditions, and privacy policies; development agreements; trademark co-existence agreements and licenses; consulting and independent contractor agreements; software licenses; and data use agreements. He also works with clients to secure domain names and has experience with proceedings under ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP), Anticybersquatter Consumer Protection Act (ACPA); and negotiations.


INTA
International
Trademark
Association