University of Chicago, Chicago Women's Alliance Presentation, "Privacy and Data Security : Is the US Business and Consumer Community Hacking it?" Presented by Stacy Baygood Streur, February 24, 2015

Privacy and Data Security For Businesses and Individuals

By: Stacy Baygood Streur, JD LLM CIPP
Streur Law, LLC
847.835.9563
sbs@streurlaw.com
streurlaw.com

Privacy and Information Security

- Privacy:
  - Information privacy
  - Bodily privacy
  - Territorial privacy
  - Communications privacy
- Information Security:
  - Methods used to prevent loss, unauthorized access or misuse of private information.
- Information security protects three aspects of the data:
  - Confidentiality
  - Integrity, and
  - Availability

Threats

- Physical
  - Infrastructure disruption/accidents
- Technical
  - Malware
  - Social engineering
  - Phishing/Spear phishing
  - Spyware
  - Spam
- Administrative
  - Intentional employee misconduct
  - Inadvertent misconduct: lost or stolen device

The Obligation to Protect Personal Information

- Federal Statutes & Regulations
- State Statues & Regulations
- Common Law
- Contractual Agreements
  - PCI DSS
  - Vendor agreements
  - Customer agreements
- Self-imposed Obligations
  - Privacy policies
  - Industry standards

US Sectoral Approach: Federal Laws

- Health Care: HIPAA and HITECH
- Financial Services: Gramm-Leach Bliley Act (GLBA) The Financial Services Modernization act of 1999;
- Children's Privacy: Children's Online Privacy Protection Act (COPPA).
- Credit Report information: Fair Credit Reporting Act (FCRA), updated by Fair and Accurate Transactions Act (FACTA);
- Consumer Private Information: FTC Act
  - Protect consumers against unfair or deceptive acts or practices

Illinois Laws:

- Illinois Personal Information Protection Act (PIPA): Disposal of Personal Information Provision
- Illinois Personal Information Protection Act (PIPA): Breach Notification Provision
- Illinois Biometric Information Privacy Act (BIPA),
- Illinois Consumer Fraud and Deceptive Practices Act Use of Social Security Numbers Provisions 815 ILCS 505/2Rr

FTC Enforcement Actions

- FTC has authority to protect consumers against unfair and deceptive trade practices.
- Almost all enforcement actions have ended in settlements, formalized by Consent Decrees.
- Two businesses have challenged FTC's authority
  - FTC v. Wyndham Worldwide
  - FTC v. LabMD

The Good News

According to the FTC:

- Business owners are not required to guarantee absolute security.

What is required: Reasonable Security .

- Security is an ongoing process of using reasonable and appropriate measures in light of:
  - The sensitivity and volume of consumer information a business holds,
  - The size and complexity of the business,
  - The cost of available tools to improve security and reduce vulnerabilities.

Best Practices for Business Owners

- FTC Recommended Best Practices
  1. Take stock
  2. Scale down
  3. Lock it
  4. Pitch it
  5. Plan Ahead

- Review your privacy policy to make sure that your statements in that policy accurately reflect your current business practices.

Additional Resources

- FTC publication , *Protecting Personal Information, A Guide for Business*, http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business;
- Ill. Atty. Gen. publication, *Information Security and Security Breach Notification Guide*, http://illinoisattorneygeneral.gov/consumers/consumer_publications.html
- Better Business Bureau publication, *Privacy Toolkit* http://www.bbb.org/council/for-businesses/toolkits/data-privacy-for-small-businesses/ does-you
- The California Attorney General, Kamala D. Harris, guidance for complying with the California Online Privacy Protection Act ("CalOPPA"). *Making Your Privacy Practices Public* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-guide- privacy-policies-and-do-not-track
- FTC v. LabMD case information, http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter

Samsung Introduced Smart TV with Voice Recognition:

Privacy Policy

- "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of voice recognition." 1.2015

Big Data: Collected from the digital world

- Big Data:
  - Collection, aggregation and processing of large data sets.
- From the digital world:
  - Online, cell phone, other computing devices.
- Collected data may be unrelated to the transaction.

Big Data: Collected from the Analog World

- Internet of Things
  - Ability of everyday objects to connect to the internet and send and receive data.
- Brick and Mortar Locations ie: Stores, Malls, and Airports collect information about you:
  - Rewards Cards.
  - Smart Phone Apps
  - Blue Tooth or Wifi signal tracking
  - Heat Pad Sensors
  - Video Survelience

What Happened to Do Not Track?

- Four years ago FTC proposed a plan to allow consumers to choose whether they wanted their online activities to be tracked or not (like do-not-call).
- Industry groups and privacy advocates (W3C) joined together to develop a system for DNT.
- Debate continues.

What do Data Brokers Do With the Information They Collect?

- Data brokers have two kinds of data:
  - Actual data
  - Derived data

- Data Brokers offer primarily three kinds of products:
  - Marketing products,
  - Risk mitigation products, and
  - People search products.

Some of the FTC Findings in Its Report on the Data Broker Industry

- Collection is from variety of sources, and largely without consumers' knowledge,
- Data is shared between brokers,
- There is collected data on nearly every U.S. consumer,
- Data is used to create scores some of which might be discriminatory,
- Online and offline data are combined.

Big Data: Benefits

- Data Broker products
  - Help to prevent fraud,
  - Improve product offerings,
  - Make targeted advertising possible,
  - Provide small businesses the ability to connect with consumers
  - Facilitate connections with old friends
- Internet of Things
  - Allows people with certain medical devices to easily work with their physician
  - Allows consumers to track their energy usage for the purpose of saving energy
  - Vehicle sensors can help notify drivers of dangerous road conditions.

Big Data: Risks

Internet of Things and Big Data Products

- Potential for unauthorized access and misuse of personal information,
- Risk to personal safety risks: ie: hacker can take over your pace maker, your home security system or your car,
- Risk that Information will be used in a discriminatory manner to make employment, credit and insurance decisions.

Big Data: Big Brother

- December 2014 Oracle announced an agreement to acquire Datalogix. (Datalogix claims to have data on 110 million US households). One stated purpose of the deal was to allow Oracle take information collected on-line and information collected off-line and combine them.
- Problem: vast majority of consumers do not want their information collected, measured, or sold.

What should be done? FTC Recommendations

May 2014: FTC Report: Data Brokers a Call for Transparency and Accountability

- Legislation to require data brokers to provide consumers access to information about them, ability correct inaccurate information and ability to opt out of use of their data for marketing purposes.
- Industry self regulation.

January 2015: FTC Report on the Internet of Things

- Legislation to address the risks and concerns but not Internet-of-Things specific legislation because of the risk to innovation.
  - General data security and breach notification legislation,
  - Strong flexible and technology neutral legislation to strengthen the FTC's currently existing data security enforcement tools.
- Industry self regulation

What Can You Do To Protect Your Personal Information?

- Read privacy policies for websites and apps and understand what information is being collected,
- Use good passwords,
- Use a security lock on your phone,
- Install security on your phone that allows you to remotely wipe the phone if you lose it,
- Use up to date anti-virus protection software,
- Encrypt personal data before storing it or sending it,
- Online you can set the browser to Do Not Track,
- Turn off your wifi and bluetooth when you are at the store or the mall,
- Some data brokers have procedure for allowing consumers to opt out of their data collection.

Additional Resources

FTC Consumer Information:

- http://www.consumer.ftc.gov/topics/privacy-identity
- http://www.consumer.ftc.gov/blog/does-your-app-know-where-you-are?utm_source=govdelivery
- http://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014
- http://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things

Privacy Rights Clearing House: Privacy Survival Guide Take Control of Your Personal Information :

- https://www.privacyrights.org

Opt out of in store tracking: Smart Store Privacy:

- http://smart-places.org/

Apple iOS 8 scrambles WiFi MAC addresses and lets you choose for each app whether you want to share information “never “ or “always.”

Thank you!

Stacy Baygood Streur, JD, LLM, CIPP
Streur Law, LLC
sbs@streurlaw.com
847.835.9563

Practice Areas: Copyright and trademark law; privacy and data security; software licensing and cloud contracts.