DATA PRIVACY/SECURITY:
Setting Your Compliance Priorities in an Era of Promised Deregulation

Linda McReynolds
CIPP/US, Of Counsel

Kara Podraza
Law Clerk

Ronald Quirk
IOT Attorney

Alex Schneider
Associate Attorney

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

DISCLAIMER: This presentation is intended for informational purposes only and is not for the purpose of providing legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a lawyer if you want legal advice. **No attorney-client or confidential relationship exists or will be formed between you and Marashlian & Donahue, PLLC, The *Comm*Law Group, or any of our representatives.**

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Goals for this Presentation

EXPLAIN: Why are we talking about privacy/data security now?

EDUCATE: What are the rules?

SET PRIORITIES: What actions can my company take to comply?

Regulatory Uncertainty

- Trump Administration Promises Deregulation
  - *Promise to eliminate two old regulations for every new regulation*
- Recent News Signals Deregulation is Here
  - *FTC enforcement agency signals to industry that it will only pursue "concrete harms" in privacy/security cases. Does this mean weaker enforcement?*
  - *FCC regulatory agency delayed data security rule implemented by Obama Administration. Congress eliminated the rest of the rules last week. FCC also pulled anticipated cybersecurity white paper.*
- On the other hand…
  - *FCC CPNI Rules remain in effect*
  - *Tough state enforcement remains*
  - *New EU regulation will have significant penalties for non-compliance*
- **Our Approach during this Session:**
  - *Highlight compliance priorities.*
  - *Suggest tools and resources your company can use now to comply with these priorities.*

WHAT ARE THE RULES?

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Overview

Enforcement Mechanisms

- **FTC:** Consumer protection agency with case-by-case adjudication
- **FCC:** Regulatory agency that promulgates and enforces rules
- **International Laws:** Privacy Shield and upcoming GDPR regulation
- **State Laws:** Privacy notice and data breach requirements

Other Authorities

- **NTIA:** Executive branch agency in the Department of Commerce
  - *Obama Administration: M*ulti-stakeholder process to develop guidelines
- **HHS:** Cabinet-level Department
  - *Enforces HIPAA:* Federal law that protects and secures patients' protected health information (PHI)
  - Business associate agreements

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

FTC: Rules to Follow

- Case-by-case adjudication of FTC Act Violations.
- Historically responsible for protecting data privacy and security
- FTC has brought more than 500 cases in which it sought to protect privacy and security of consumer information.
- The "Common Carrier" Exemption: 2015 Open Internet Order mandating Net Neutrality turned ISPs into "common carriers." FTC cannot oversee "common carriers."
  - *Created an ISP privacy loophole.*

Focus of the FTC

- Data Privacy
  - *Issued a report containing best practices for businesses to protect the privacy of consumers and give them greater control over the collection and use of their personal data.*
  - *The goal is to balance the privacy interests of consumers with innovation that relies on information to develop beneficial new products and services.*
- Data Security
  - *Issued some recommended best practices for IoT device manufacturers in order to mitigate the possibility of legal violations.*
    - i.e. Security by design, security risk assessments, security testing measures and security personnel practices.
- Examples of Potential Claims:
  - *Making false claims on collection, use, sharing of consumer data*
  - *Failing to provide reasonable security for consumer data*
  - *Deceptively tracking consumers online*
  - *Spamming and defrauding consumers*

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

FTC: Examples of Practices to Avoid

- FTC Enforcement Examples
  - *Turn, Inc.:* Tracked consumers both online and through their mobile devises. FTC settled case and ordered company to implement new compliance program. Any violation of the order could result in a fine up to $40K per incident.
  - *InMobi:* Illegally tracked hundreds of millions of consumers' location (including children) without their consent. Company paid $950K in civil penalties and was ordered to implement comprehensive privacy program.
  - *ASUSTeK Computer, Inc.:* Provided insecure home routers and "cloud" services. FTC ordered company to establish and maintain a security program subject to audits for the next 20 years
  - *Vizio, Inc.* Collected information from TVs without consumers' knowledge or consent. Will pay **$2.2 million** to settle.

FCC: Rules to Follow

- Upheaval since October 2016
- Longstanding Customer Proprietary Network Information (CPNI) Rules
  - *Section 222 of the Communications Act: Congress' word on telecom privacy*
  - *Since 2007, rules have applied to interconnected VoIP service providers*
  - *CPNI: Customer information obtained by a telecom provider during the course of providing service to a customer.*
  - *Easiest description: WHERE, WHEN, and TO WHOM a customer places a call (i.e. Call Detail Records)*
  - *NEVER included personally identifiable information (i.e. phone number, address, customer name); NEVER included sensitive personal information, such as SSN or account numbers; NEVER included the content of communications.*
  - *Rules: Obtain consent (usually opt-out every 2 years), provide notice, reasonably protect CPNI, and report any breach of CPNI.*
- Goals
  - *Limits Marketing: Can protect customers from telemarketers looking to win back a customer or upsell them.*
  - *Pretexting scandals (unauthorized access to records.) CPNI rules mandate identity verification procedures.*
- *Status of annual certificates of compliance*

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

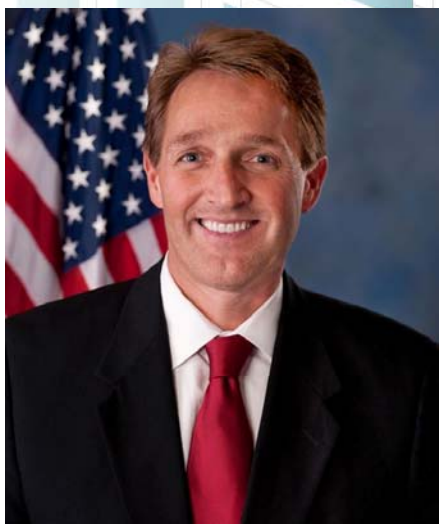
New FCC Privacy Rules

- In March 2016, the FCC proposed new privacy rules. After extensive comment period, new rules were implemented in October 2016.
- Applied to Traditional Telecom Providers, Interconnected VoIP providers, and to ISPs.
- Controversial: ISPs had never had special privacy rules applied to them.
  - *Net Neutrality / Open Internet Order: FCC began regulating ISPs as common carriers.*
  - *Now ISPs would have privacy rules; but regular internet companies like Google and Facebook would not.*
  - *Also: FTC cannot regulate common carriers. FCC decided to use its Section 222 and begin regulating ISPs.*
- Implementation: Would be implemented over the course of one year.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

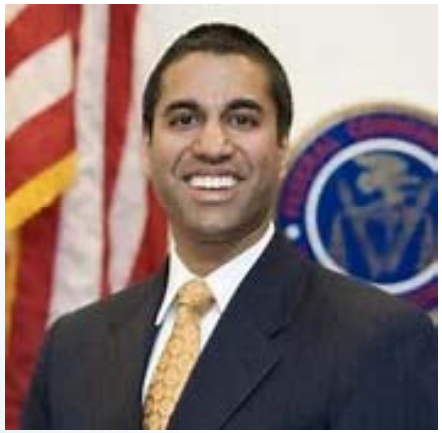
Efforts to Abandon New FCC Rules

Sen. Jeff Flake (R-AZ)



- Introduced a resolution to eliminate the FCC's privacy rules through the Congressional Review Act.
- Passed in both the Senate (50-48) and the House (215-205) on mostly party lines.

FCC Chairman Ajit Pai



- Stated he will work to establish a "technology-neutral" privacy framework.
- Praised the recent Congressional vote, declared his goal of returning jurisdiction over broadband providers' privacy practices to the FTC.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Data Covered by FCC Rules

Currently Covered:

- **Traditional CPNI**: Data about a call, e.g. Call Detail Records.

Also:

- **ISP CPNI**: Data about internet usage, e.g. domains visited, traffic statistics, and information about the subscription of the customer.
- **Content of communications and other data:** Contents of emails or messages, and items viewed, read, watched, searched, selected.
- **Personally identifiable information (PII):** Customer contact and biographical information.

The Abandoned FCC Rules

- **Notice**: Describe & explain the purpose of any collection, use, or sharing of customer PI.
- **Choice**: Obtain "opt in" consent to share or use Sensitive Customer Data. Obtain "opt-out" consent for other types of data. Inform customers on how the information will be used and create a mechanism to revoke consent.
  - *Sensitive: Financial information, health information, SSNs, precise location, children's information, content of communications, call detail records, customer web browsing history & app usage history.*
- **Data Security: Reasonable** data security practices.
- **Data Breach Notification**: Notify FCC & Customers, as well as law enforcement.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

THE FCC RULES ARE GOING AWAY. SO, WHAT SHOULD MY COMPANY BE THINKING ABOUT ***NOW***?

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

International Regulation: Privacy Shield

US	**EU**
No overarching privacy law (Market Focused)	Data Protection Directive and E-Privacy Directive (Rights Focused)
Few federal laws, state provisions, and administrative regulations (FCC, FTC) for data protection	Sets out specific provisions and rights for personal data, including collecting data for only a legitimate purpose.

Coming Together: EU-U.S. and Swiss-U.S. Privacy Shield Framework

- *Mechanism to provide companies a way to comply with data protection requirements between the EU and Switzerland to the U.S.*
- *Administered by the International Trade Administration in the U.S.*
- *Voluntary framework, but binding once commitment is made*

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

International Regulation: GDPR

- General Data Protection Regulation (will replace Directive 94/46/EC)
- Main Subjects Covered:
  - *Breach Notification, Right to be Forgotten, Right to Access, Data Portability, Data Minimization, and Data Protection Officers*
- Major Implications:
  - *Extra-territoriality:* Applies to companies processing personal data of customers residing in the EU, regardless of company's location.
  - *Consent Strengthened:* Consent options must be provided in a clear and easily accessible form, inform the purpose for using the data, and be easy to withdraw.
  - *Penalties:* Tiered approach to fines on global revenue.
    - Maximum fine: 4% of annual global revenue or €20 Million
- Effective: **May 25, 2018**

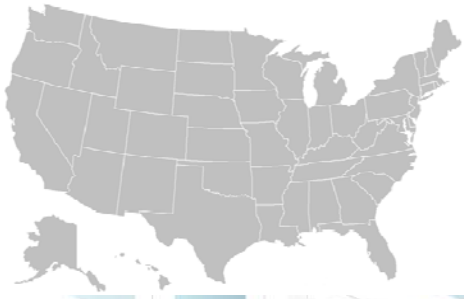
MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

HIPAA

- Who is a Covered Entity?
  - *Health plans (i.e. health insurance companies), a majority of health care providers, and health care clearinghouses.*
- What Information is Protected?
  - *PHI: Information from doctors, nurses, and health care providers, billing information, conversations between medical professionals, etc.*
- What are the rules?
  - *Privacy Rule:* Sets limits and conditions on uses and disclosures that can be made without authorization. Gives patients certain rights over their PHI.
  - *Security Rule*: Requires appropriate administrative and technical safeguards to ensure the security of electronic PHI.
- Enforcement: Business Associate Agreement
  - Covered entities must enter into a Business Associate Agreement with any business associates or PHI cannot be shared.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

State Laws



- Even with uncertainly after elimination of FCC rules, state laws remain effective.
- Recent *NY Times* Article: States are responding to federal government deregulation by creating their own privacy laws.
  - *"Federal blockage can create local opportunities."*
  - *California, Connecticut, Illinois, New Mexico, etc.*
  - *Proposed Illinois law - "Right to know": Let consumers know what information about them is being collected by companies*
    - If passed, this rule could serve as a model for other states
- Minnesota Senate: Voted on 3/29 to bar ISPs from selling users' personal data without express written consent.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Outside Influences

- Often overlooked: Role of non-governmental, non-industry advocates and media groups.
- Consumer Reports: Long subjected vacuum cleaners, cars, and washing machines to rigorous tests. What about privacy?
- New standards:
  - *Products should be build to be secure (think security by design, default passwords)*
  - *Products should preserve consumer privacy*
  - *Products should protect the idea of ownership (alter, fix, or resell products purchased)*
  - *Act ethically (i.e. consider customer perspective)*
- Customer goodwill

WHAT ACTIONS CAN YOUR COMPANY TAKE?

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Privacy Notices

- **State Regulations:** States have their own privacy policies that are enforced regardless of the FCC's current and future rules.
  - *Ex. California Online Privacy Protection Act*
    - Requires website operators to include a privacy policy linked to its homepage stating exactly what information is collected and who it is shared with.
- **International Regulations:** GDPR
  - *Provide transparent and easily accessible policies in an intelligible form.*
    - Using clear and plain language, adapted to the data subject.
- **Industry Guidelines:** Standard practice to provide notice on what you collect, how information is used, when will be shared with third parties.
  - *CRITICAL to follow through with your promises.*

Choice

- **FTC Guidelines:** Follow best practices to avoid enforcement actions.
- **Industry Practices:** Opt in for sensitive data, opt-out for non-sensitive personalized third party marketing. Rely on Implied Consent for: service fulfillment and support, fraud prevention, market research, product development, network management and security, compliance with law, and first party marketing.
  - ***PRIORITY:*** *Consider the costs/benefits of building into your online portal a consent mechanism for customers to grant and revoke consent. Why?*
    - Increasingly an industry standard practice
    - Customer goodwill
- **Existing FCC Requirements:** The CPNI rules are the FCC's original privacy enforcement mechanism. Ensure you have a CPNI compliance plan.
- **International Requirements:** GDPR
  - Provide information about where and what purpose individual data will be used for.
  - Must obtain specific, informed and explicit consent by statement or action signifying agreement.
    - Consent can be withdrawn at any time.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Data Security

- "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information …"
- FCC Enforcement: *TerraCom, Inc.* and *YourTel America, Inc.*
  - *Failed to protect customer PI by disregarding reasonable security measures, claiming customer PI was protected when it was in fact stored on unprotected servers, and failing to inform customers that their PI was compromised by third-party access.*
  - *Resulted in $10 million forfeiture.*
- **Result:** Companies must consider appropriate and reasonable security measures in order to protect their customers from unacceptable risk and harm.

Data Security Best Practices

- Best Practice to Consider:
  - ☑ *Engage with available industry best practices & risk management tools.*
  - ☑ *Develop a written data security compliance program.*
  - ☑ *Designate a privacy officer with responsibility over the practices.*
  - ☑ *Train employees & contractors to properly handle customer data.*
  - ☑ *Promote safe handling of data shared with third parties.*
  - ☑ *Implement strong customer authentication techniques.*
  - ☑ *Practice minimization: collect only necessary information, retain as needed, and dispose of properly.*

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Data Breach Notification

- **State Requirements:** *47* states have enacted legislation requiring private or government entities to notify individuals of data breaches.
  - *States have enacted laws addressing:*
    - Who must comply
    - What constitutes personally identifiable information
    - What constitutes a breach
    - What type of notice should be provided
- **International Requirements**: GDPR
  - Breach notification becomes mandatory in all member states where data breach is likely to "result in a risk for the rights and freedoms of individuals."
  - Must be done within 72 hours of breach – notify customers without delay

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Data Breach Notification

- Considerations for breach or potential breaches:
  - *Create and send out a prompt and detailed customer notification*
    - Include any important information, such as date, details of the breach, and contact information.
  - *Notify the prospective law enforcement agencies or the FCC as required by rules or laws.*
  - *Keep a record for <u>at least</u> 2 years after the data breach.*

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Actions to Take Now

- **Assessments of Risk:** Develop a compliance plan
  - Thoroughly consider all possible risks presented by your company's collection and retention of customer data.
  - Confirm that your data security practice meet all of the applicable regulatory and international standards.
- **Best Practices:** Engage in best practices from FCC, NIST, & FTC
  - Ensure consistency between your Privacy Notice and data security practices, implement strong data authentication, etc.
- **Contracts:** Review and Revise Third Party Contracts
  - Pay attention to covered data flows involving CPNI, PII, or the content of communications.
- **Plan Ahead:** Plan to meet FCC/GDPR implementation deadlines. Follow policy/regulatory developments and rule changes.
- **Privacy Officer/Outside Attorney:** Implementation of compliance plan, privacy priorities.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Risk Assessment Package Plan

- The *Comm*Law Group's Privacy Practice offers a **fixed-fee,** privacy risk assessment service. We'll help you sort out the first steps to ensuring compliance with applicable laws and regulations:
  - *Review your current practices;*
  - *Identify applicable laws and regulations;*
  - *Develop a plan to shore up privacy and data security practices and defenses; and*
  - *Provide a candid assessment of risk based on our knowledge of the agencies and laws at issue.*
- Please email The *Comm*Law Group's Privacy Practice Chair Linda McReynolds, CIPP/US, at lgm@commlawgroup.com to get started.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

PRIVACY AND DATA SECURITY ARE ***NOT*** GOING AWAY.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP

Questions?

If you have any questions regarding implementation, you may consider hiring a privacy attorney who knows FCC compliance.

We can help your business build a long term plan to achieve ongoing compliance with the FCC's new privacy rule.

To learn more, please contact The *Comm*Law Group's Privacy Practice Chair Linda McReynolds, CIPP/US, at lgm@commlawgroup.com, or 703-714-1318.

MARASHLIAN & DONAHUE, PLLC
THE COMMLAW GROUP