



# FCC Privacy Rules for Broadband Providers and their Impact on Publishers

Natasha Kohne

November 17, 2016

## Privacy & Security Landscape and Trends

- 2016: The Year of Landmark Privacy Rulings
- Increased activity in privacy and security regulatory space
  - EU GDPR
  - Safe Harbor / Privacy Shield
  - New York Department of Financial Services
- Expanding definition of sensitive, personal information
  - Geolocation
    - FTC, courts, state legislatures
  - IP Addresses
    - FTC, courts, CJEU
- Establishing basis for more intangible harms (Spokeo)
- Snowball Effect or End of the Road?

## Overview of New Rule

- FCC's 2015 Open Internet Order reclassified broadband as a Title II common carrier service
- FTC cannot regulate common carriers
- This reclassification led to the issuance and adoption of new privacy and data security rules
- Proposed rule issued in April 2016
- Approximately three months of public comments
- Total six months of internal discussion and public comment
- Received a quarter of a million filings
- Final rule approved in October 2016 and released on November 2, 2016
- New version was "scaled-back"
- Approved by 3-2 split, along party lines

## Proposed Rule v. Final Rule

Proposed Rule	Final Rule
PII defined as any information that is linked or linkable to an individual	PII is defined as information that is linked or reasonably linkable to an individual or device
Opt-in consent based on type of entity	Opt-in consent based on sensitivity of information
Imposes strict liability on companies for ensuring security	Imposes a reasonable security standard
Notification of a breach based on unauthorized access to <i>any</i> customer proprietary information	Notification of breach based on unauthorized disclosure of customer's personal information
Notice to consumers within 10 days	Notice to consumers within 30 days

# Commissioners' Comments

## Democratic



*"Today, the Commission takes a significant step to safeguard consumer privacy in this time of rapid technological change, as we adopt rules that will allow consumers to choose how their Internet Service Provider (ISP) uses and shares their personal data. The bottom line is that it's your data. How it's used and shared should be your choice."*  
Chairman Tom Wheeler



*"This is real privacy control for consumers. It helps in the here and now. But with respect to the future of privacy, I think we still have work to do. . . . I think it is time for a 21st century inter-agency privacy council."*

Commissioner Jessica Rosenworcel



*"Today, we substantially adopt the FTC's framework on privacy, with some tweaks to account for the current era, and unique position broadband providers occupy in our everyday lives. Where we deviate, we do so with the protection of consumers in mind."*

Commissioner Mignon Clyburn

## Republican



*"Nothing in these rules will stop edge-providers from harvesting and monetising your data, whether it's the websites you visit or the YouTube videos you watch or the e-mails you send."*  
Commissioner Ajit Pai



*"[T]he FCC quickly embarked on an expansionist mission, seeking to impose situationally-defective new requirements that are stricter than most consumers would ever want or expect and that exceed the Commission's authority."*  
Commissioner Michael O'Rielly

## Features of the New Rule – Privacy

### ■ Transparency

- ISPs must give consumers clear **notice** about what types of information the ISP collects about its customers; specify how and for what purpose the ISP uses and shares this information; identify the types of entities with which the ISP shares this information.
- Notice must be both “immediate and persistent”.

### ■ Consumer Choice: Opt-In Consent

- ISPs must obtain **opt-in consent** from their customers to use and share “**sensitive**” **personal information**: precise geo-location, health information, children’s information, financial information, social security numbers, web browsing history, app usage history, and the content of communications.

### ■ Consumer Choice: Opt-Out Consent

- An ISP’s use and sharing of **non-sensitive personal information**, such as email addresses and service tier information, will generally be subject to customer’s **opt-out consent**. Consent will not be required in some cases, such as when information is used to provide the broadband service.

## Features of the New Rule – Privacy

### ■ De-identified Information:

- ISPs may use and share de-identified information without obtaining consent, provided that they (1) take specific steps to ensure the information cannot be reasonably linked to a specific individual/device, (2) publicly commit to not attempt to re-identify information, and (3) contractually prohibit the re-identification of shared information.

### ■ Take-It-Or-Leave-It Offers:

- ISPs cannot refuse to serve customers who don't consent to the use and sharing of their information for commercial purposes.

### ■ Pay for Privacy:

- If it chooses to offer a discount or other incentive in exchange for customer content/opt-in consent, an ISP must comply with heightened disclosure requirements. The FCC will evaluate the legitimacy of such programs on a case-by-case basis.

## Features of the New Rule – Data Breach Notification

- In the event an ISP “reasonably determines” that **unauthorized access to, use, or disclosure of a customer’s personal information** has occurred, unless the ISP determines that **no harm is reasonably likely to occur**, the ISP must notify:
  - Affected customers without unreasonable delay and no later than 30 days after the determination has been made;
  - The FCC, which shall receive notification of all breaches that meet the harm-based trigger,
    - **Fewer than 5,000 customers:** without unreasonable delay and no later than 30 calendar days following the determination
    - **5,000 or more customers:** within 7 business days of the determination and at least 3 days before notifying customers
  - The FBI and Secret Service, if the breach affected 5,000 or more customers, no later than 7 business days after the determination has been made and at least 3 days before notifying customers
- There is a **rebuttable presumption** that any breach involving sensitive customer PI poses a reasonable likelihood of customer harm and would therefore require customer notification.



## Features of New Rule – Security

- “[A] provider must adopt security practices appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility”
- Consistent with FTC and NIST
- No prescriptive checklist

### **Practices that are exemplary of reasonable data security:**

- Engagement with industry best practices and risk management tools
  - Industry best practices; NIST CSF; Guidance from the FTC; CSRIC best practices
- Strong accountability and oversight
  - Written comprehensive data security program; senior management official(s) with responsibility over data security practices; employee / contractor training; data security commitments from third parties
- Robust Customer Authentication
  - Periodic reassessment of the efficacy of authentication practices; notify customers of account changes and attempted account changes
- Other practices
  - Data minimization; FTC Disposal Rule; strong data encryption; information sharing practices

## Previous Data Security Enforcement Actions

- FCC brought three enforcement actions, collecting roughly \$30 million in fines between 2014 and 2015
  - Highest fine: \$25 million
- TerraCom, Inc./YourTel America, Inc., AT&T and Cox Communications
- Settlement agreements required privacy and security improvements, including:
  - Conduct privacy **risk assessments**
  - Using a risk-based approach, implement and maintain a **written information security program** to protect the security, confidentiality, and integrity of PI and CPNI collected and/or maintained
  - Implement and maintain an **incident response plan** that it is reasonable and comprehensive
  - Implement **multiple-factor authentication** for remote access for employees as well as third parties that have access to the company's PI/CPNI
  - Maintaining reasonable **oversight of third party vendors**
  - Provide privacy and security awareness **training** to employees
  - Conduct **annual penetration testing** of systems and processes related to payment cards and collection and storage of PI/CPNI
  - Develop procedures for **internal threat monitoring** that include detection of anomalous conduct by employees
- Why hasn't the FCC brought any further cases?

## Areas of Scrutiny

---

- Pay for privacy
- 7 days from “determination”
- Harmed-based notification trigger to include financial, physical and emotional harm
- Combination of non-sensitive data could be considered sensitive
- Binding Mandatory Arbitration Rule – February 2017
- Lack of harmonized rules among players in the internet ecosystem

## Looking Ahead

### ■ Implementation

- The data security requirements become effective 90 days after the final rules are published in the Federal Register.
- The breach notification requirements become effective 6 months after publication.
- The notice and choice requirements become effective one year from publication (two years for smaller providers).

### ■ Trump administration

### ■ Possible postponement of implementing rule

### ■ Congress and Commission to revisit reclassification and net neutrality rules next year

### ■ Uniform Federal Privacy Rule?

### ■ Legal Challenges?

■ Questions?