PRIVACY OPPORTUNITIES ABOUND

CPNI, Red Flag, Broadband

TSTCI Accounting and Marketing/Customer Service Conference

July 12-14, 2017

PRIVACY – A HUGE ISSUE

In the News

- Over 200 news stories from Reuters on privacy in 2017
- Recent headlines:
  - *A judge threw out a lawsuit alleging Facebook tracks logged out users*
  - *WannaCry attack shows trend toward 'economic' cyber threats, rising regulatory risk*
  - *Google Will No Longer Scan Gmail for Ad Targeting*
  - *Facebook Gets Slap on the Wrist from 2 European Privacy Regulators*
  - *How Privacy Became a Commodity for the Rich and Powerful*
  - *Chipotle says hackers hit most restaurants in data breach*
  - *Colleges offer cybersecurity programs to fill jobs gap*

The Repeal of Online Privacy Protections

- Media frenzy over Congressional action on new broadband privacy rules
  - "The new F.C.C. rules would have given consumers stronger privacy protections — without such restrictions, internet providers may decide to become more aggressive with data collection and retention. Expect more targeted advertising to come your way."

FCC/FTC Response

"**No, Republicans didn't just strip away your Internet privacy rights"**
By Ajit Pai and Maureen Ohlhausen

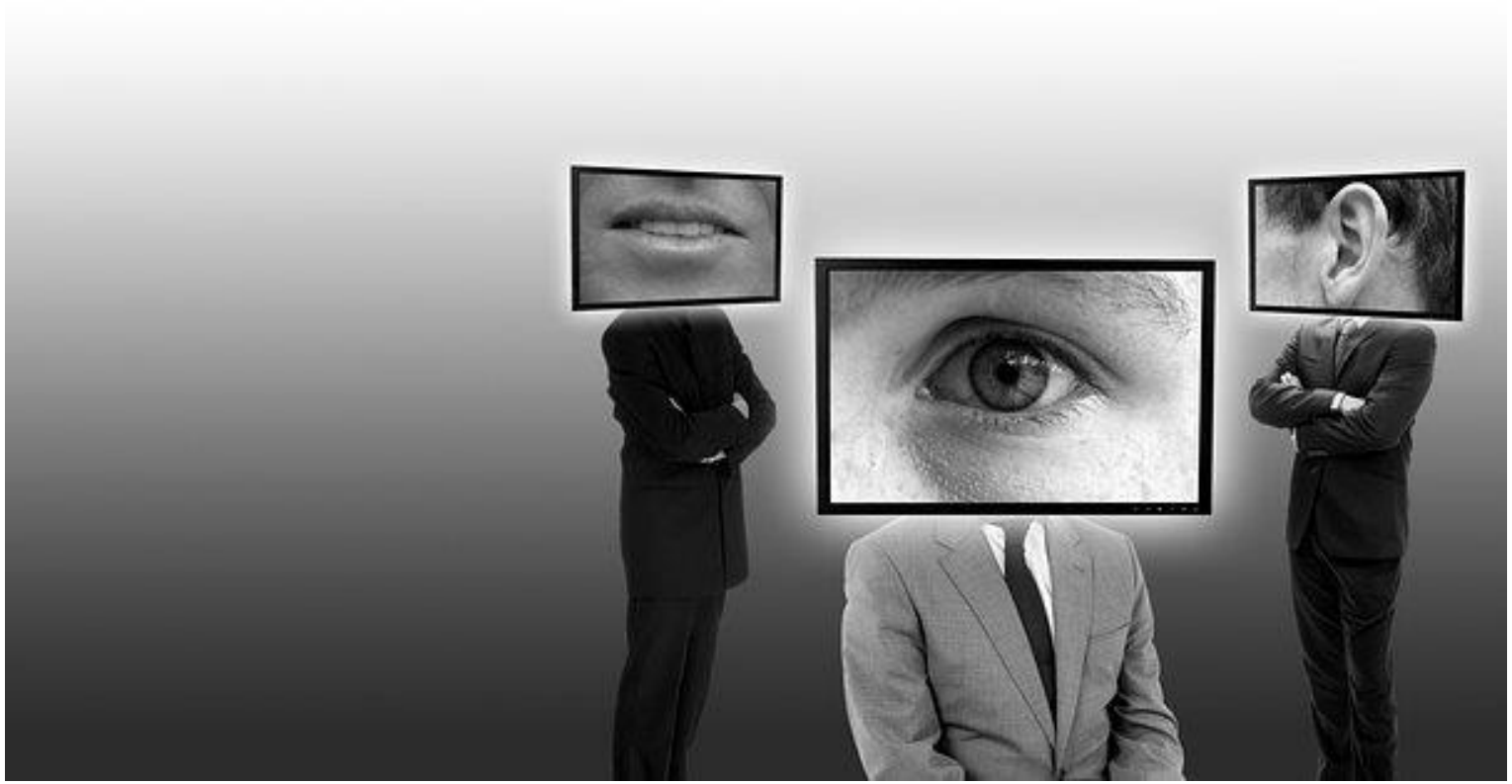
Three Main Considerations

What do our customers think, want and need?

How can we give our customers what they want and maybe make some money too?

How can we comply with industry mandates/best practices?

What Your Customers Think



What Your Customers Think

"I share data every time I leave the house, whether I want to or not. Every time I use a credit card, every time I walk in 80% of the commercial establishments in the nation, every time I drive down streets in most any city or town in the nation, I'm being recorded in some fashion. The data is there, and it's being used, and there isn't a damn thing most of us can do about it, other than strongly resent it. The data isn't really the problem. It's who gets to see and use that data that creates problems. It's too late to put that genie back in the bottle."

Customer Privacy Research

- Privacy Annoyances
  - Feeling of hopelessness or resignation
  - How hard it is to figure out what is collected and by whom
  - Uncertainty about how data is being used
  - Lack of private places

Privacy Trade-offs

- Trade-off CONS
  - Unwanted emails/contact
  - Vulnerability to scams and hacks
  - Challenges keeping location data precious
  - Profiling is "creepy"
  - Ulterior motives for data
- Trade-off PROS
  - Free stuff
  - Easy commercial and social interactions
  - Increased safety in certain circumstances
  - Increased functionality (such as with smart home products)

Privacy Trade-offs

Retail loyalty cards

- 47% “acceptable”
- 20% “it depends”
- 32% “not acceptable”

Auto Insurance

- 37%
- 16%
- 45%

Smart thermostat

- 27%
- 17%
- 55%

What Experts Say

THE FUTURE OF THE INTERNET | THE INTERNET OF THINGS

"Despite hacks and privacy issues, people will feel a need to keep connected, partly because companies will reward them for doing so (or make life difficult if they don't). People will feel resigned to navigating an environment where data are key coins of exchange."

— JOSEPH TUROW, A COMMUNICATIONS PROFESSOR AT THE UNIVERSITY OF PENNSYLVANIA

PEW RESEARCH CENTER

What Experts Say

THE FUTURE OF THE INTERNET | THE INTERNET OF THINGS

"Despite continued security problems, the IoT will spread and people will become increasingly dependent on it. The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive."

— RICHARD ADLER, DISTINGUISHED FELLOW AT THE INSTITUTE FOR THE FUTURE

PEW RESEARCH CENTER

Customer Info Wrap Up

Customers are hearing about privacy everywhere

Customers are annoyed with lack of privacy, but continue to avoid measures to protect it

They like their privacy, but are willing to share some data for something in return

Customers are purchasing more and more IoT products, which are creating meaningful data and contributing to lack of privacy

What Can We Provide Our Customers?

Privacy Services in the Marketplace

- AT&T might start charging customers to keep their data private
  - "As the privacy revolution evolves, I think people are going to want more control, and maybe that's the pricing model that's ultimately what consumers want" - AT&T's Senior VP Robert Quinn

Privacy Services in the Marketplace

- Verizon's Digital Security Products
  - This suite of products combines traditional device-based security, identity theft protection and advanced parental controls
  - **Internet Security Powered by McAfee - $10/mo**
    - Virus and malware detection and removal
    - Protect unlimited devices
    - Warn users of risky websites
    - Neutralize bad apps

Privacy Services in the Marketplace

- Verizon's Digital Security Products (Cont'd)
  - LifeLock Select - $9/mo.
    - **LifeLock Identity Alert® System**
      Monitors for fraudulent use of your social security number, name, address or date of birth in applications for credit and services.
    - **Fictitious identify monitoring**
      Scans for names and addresses connected with your social security number to help protect against criminals building fictitious identities to open accounts or commit fraud
    - **Checking, savings, credit card monitoring and alerts**
      Helps protect your finances from fraud with alerts that notify you of cash withdrawals, balance transfers and large purchases
    - **Lost wallet protection**
      Call LifeLock if your wallet is lost or stolen for help canceling or replacing credit cards, driver's licenses, social security cards, insurance cards and more
    - **Million Dollar Protection™ Package**
      LifeLock helps protect you with reimbursement for stolen funds and compensation for personal expenses as a result of identity theft based on the limits of your plan and provides legal and expert assistance if needed with our Service Guarantee

Privacy Services in the Marketplace

- Verizon's Device Protection Plans
  - Basic - $9.99/mo.
    - **Coverage for old and new devices**
      All laptops, tablets, netbooks, desktops and eligible accessories
    - **Simple claims**
      No device registration. Submit a claim 24/7
    - **Accidental damage from handling**
      Coverage for damage resulting from spills, falls, cracks, and handling*
  - Premium – Additional $19.99/mo.
    - Includes protection for TVs and gaming consoles

Privacy Services in the Marketplace

- Windstream

SECURITY PACK

Get more security for less.

- Online Backup storage of up to 100 GB
- Remote IT Support on up to 10 devices
- McAfee Security

Starting at $10.00/mo

Privacy Services in the Marketplace

- CenturyLink's @Ease Standard

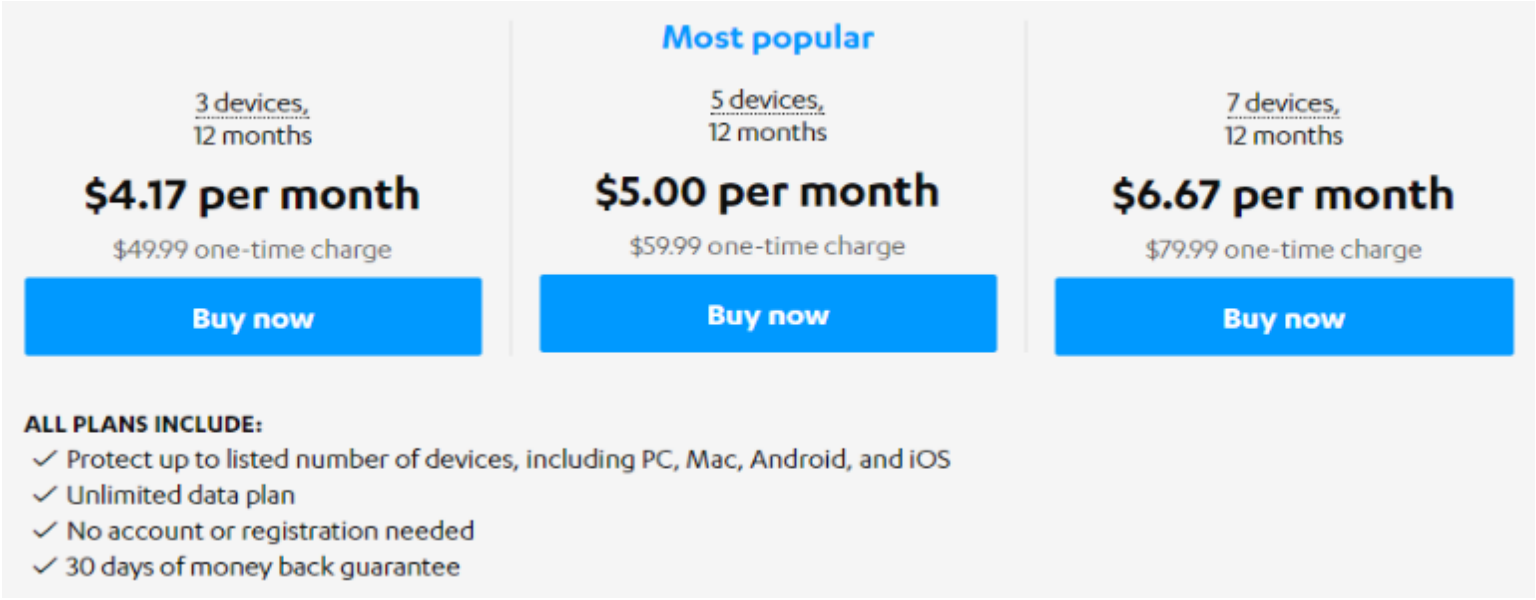
Benefits / Package	Basic	Standard $9.99/mo	Advanced $14.99/mo	Ultra $19.99/mo
PC Security (by Norton)	AntiVirus	Internet Security	Norton 360	Norton 360
PC Protection (repair/replacement)		✓	✓	✓
Inside Wire Coverage		✓	✓	✓
Online Backup (by Norton)		5 GB	50 GB	200 GB
PC Services (enhanced support)		Level 1	Level 2	Level 3
Lifetime Modem Warranty			✓	✓
Identity Theft Protection				✓

Privacy Services in the Marketplace

- Spectrum's Security Suite – included with Internet
  - McAfee® Antivirus Software: Guard against viruses and online threats
  - Firewall Protection: Blocks access to suspicious activity from hackers and malware
  - Global Threat Intelligence: Protects customers against cyber threats across all vectors — file, web, messaging and network
  - Web Advisor: Browsing protection to avoid risky websites and downloads
  - Parental Controls: Manage your children's PC and content

Privacy Services in the Marketplace

- Paid Virtual Network Service
  - Connect directly to you VPN (ISP will see this connection), and then all Internet browsing goes through the VPN's servers and blocks third parties from viewing information.



Privacy Services in the Marketplace

Other

- Alternative browsers
- Browser extensions
- File level encryption services
- Malware monitoring services
- Reputation defender/Identity theft protection services

Can/Should We Mine Customer Data?

Both personal customer data and aggregate data are valuable

- Personal data
  - Directed advertising is profitable
- Aggregate data
  - Aggregated data and anonymous data have value for use in AI and machine learning

Differences in Data Harvesting

Edge Providers	ISPs
• Harvest information when at website or using application • Free services offered in exchange for allowing data to be used • Regulated by FTC	• Able to harvest all activities that are unencrypted • Most have captive customers • Customers pay for service • Regulated by FCC (Sort of, for now)

AT&T Privacy Policy

- AT&T may collect
  - IP addresses
  - URLs
  - Data transmission rates and delays
  - Webpages you visit
  - Time spent on pages
  - Links or ads you see and follow
  - Search terms you enter
  - How often you open an application
  - How long you spend using an application
  - Other similar information

Online Behavioral Advertising

- AT&T and its advertising partners may use
  - Anonymous information gathered through cookies and similar technologies
  - Other anonymous and aggregate information useful to tailor ads shown on non-AT&T sites
  - Activities are part of "relevant advertising"

Privacy Service Info Wrap Up

Lots of services available in the marketplace that may serve as inspiration for ISP product expansion

ISPs are well positioned as tech experts in rural communities; good fit for providing security/privacy services

Customer data can be valuable and could open doors to other revenue opportunities

Must ensure that new products help customers and don't further annoy

Complying with Privacy Rules

Privacy Rules Timeline

- Pursuant to Section 222, FCC adopted CPNI rules in 47 CFR § 64.2001-2011 that applied to voice communications (telecom & VoIP)
- May 20, 2015, FCC released an Enforcement Advisory stating that Section 222 would apply to broadband and FCC would enforce
- Effective June 12, 2015, FCC Open Internet Order Applied Section 222 to Broadband Internet Access Service (BIAS)
- Nov. 2, 2016, FCC adopted CPNI rules for BIAS
- March, 2017, U.S. Congress overturned Nov. 2, 2016 CPNI rules for BIAS
- June 29, 2017, FCC issued order clarifying CPNI rules for voice and reminding ISPs that BIAS is subject to Section 222

CPNI/Privacy Rules in Effect Now

47 CFR § 64.2001-2011	• Voice-centric rules applying to telecom and VoIP
Statutory Provisions of Sections 201, 202 and 222	• Applies to both voice and BIAS
Other	• FTC's NIST Framework • State rules and regs

FCC Actions

- FCC and Congress are intent to regulate ISPs similar to edge providers via the FTC
- This approach matches with Pai's goal to roll back the Open Internet Order
- FCC would never have Title II regulation over edge providers to control privacy of data

Privacy Protections Broader Than Just CPNI

- Section 222(a) contains a broad, general requirement that every telecommunications carrier has a duty to protect the confidentiality of its customers' Proprietary Information (PI)
- Section 222(b) pertains to PI exchanged between carriers
- Section 222(c) pertains to Customer Proprietary Network Information (CPNI)

  - CPNI has the greatest level of protection and imposes restrictions on carriers' ability to use, disclose, or permit access to customers' CPNI without their consent

Guidance from Enforcement

Open Internet Order cites TerraCom & YourTel decision as an example of how it takes enforcement of Section 222 "seriously"

PI was submitted by applicants for the companies' Lifeline offerings on electronic application forms to establish proof of eligibility

Companies collected this information through their websites and the PI was stored on dedicated data servers provided by a third party vendor, Vcare

An investigative reporter working for Scripps discovered that the PI was being stored on an unprotected Internet site and was able to locate a consumer's PI by conducting a Google search

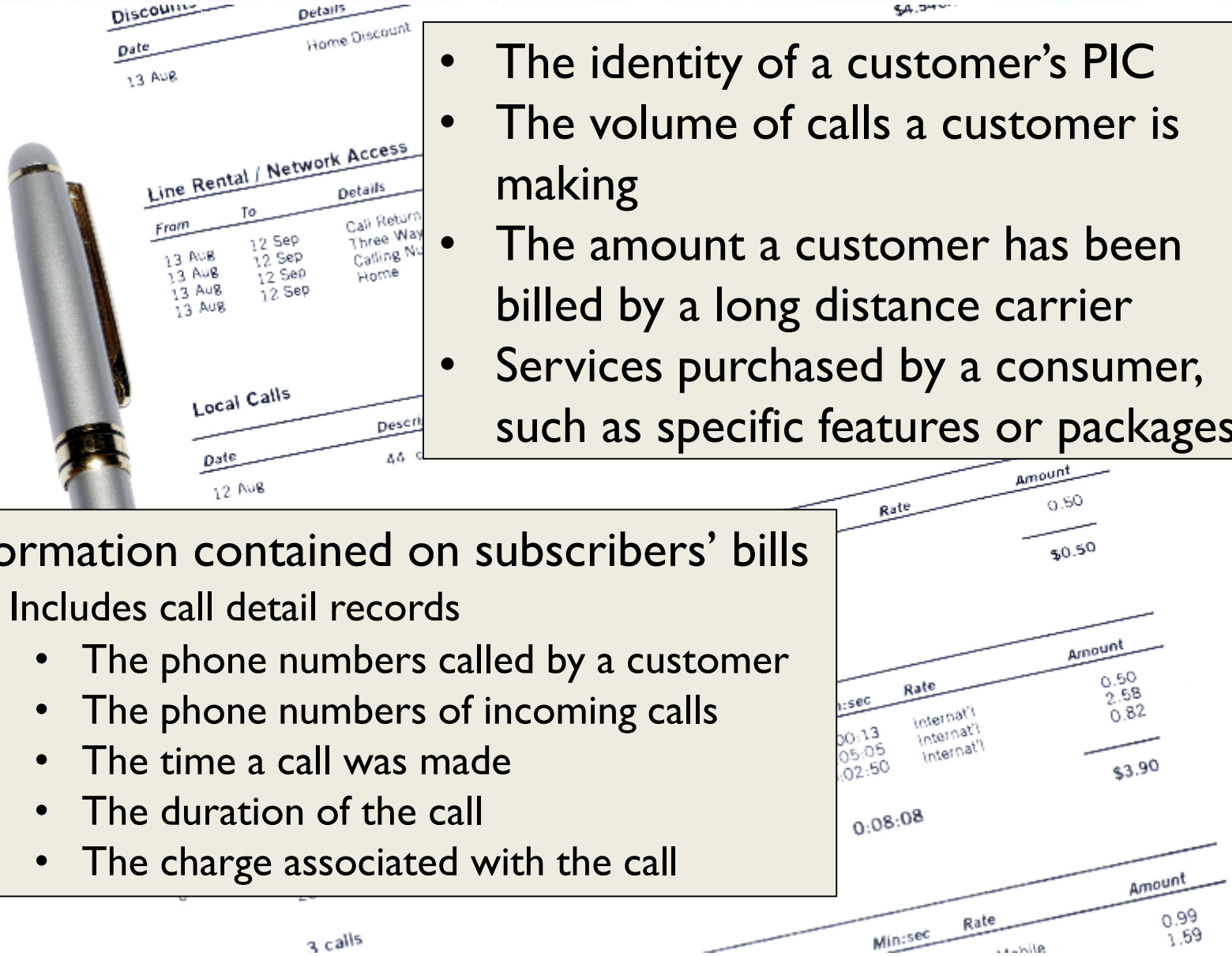
After the reporter notified the companies, the companies notified the Enforcement Bureau claiming that they were victims of a security breach

Guidance from Enforcement

FCC also found the Companies had violated Section 201(b)

- Failing to employ reasonable data security practices to protect consumers' PI
- Representing in their privacy policies that they protected customers' personal information, when in fact they did not
- Failing to notify all customers whose personal information could have been breached by the Companies' inadequate data security policies (cites encryption & URL naming convention)

Examples of Voice CPNI



- The identity of a customer's PIC
- The volume of calls a customer is making
- The amount a customer has been billed by a long distance carrier
- Services purchased by a consumer, such as specific features or packages

- Information contained on subscribers' bills
  - Includes call detail records
    - The phone numbers called by a customer
    - The phone numbers of incoming calls
    - The time a call was made
    - The duration of the call
    - The charge associated with the call

What is Not Considered CPNI

Customer's Name, Address and Phone Number

- FCC ruled that carriers may contact all of its existing and/or former customers for marketing purposes using a list containing the customers' names, addresses and telephone numbers so long as it does not use CPNI to select a subset of customers from that list

CPNI – When You CAN Use It

For billing and collection or to otherwise provision ordered service

To include subscriber list information in a directory (unless customer requests unlisted)

To protect the rights or property of the carrier, or to protect users and other carriers from fraudulent, abusive, or unlawful practices

To market service offerings that are part of the telecom service or package of services to which the customer already subscribes

Upon affirmative written request by the customer, to any person designated by the customer

With customer approval (opt-in, opt-out, or single use), when marketing services outside of the telecom service or package of services to which the customer subscribes

Opt-In/Opt-Out Approval

Opt-In

- Opt-in must be used if carrier wants to share CPNI in a joint venture arrangement
- Requires that the carrier obtain customer's affirmative, express consent

Opt-Out

- Only required for voice service if target customer does not already subscribe to voice product
- Customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object within the specified waiting period
- Waiting period is 30 days; 33 days if notice is mailed

Streamlined Approval for One-Time Use

- A telecom carrier may orally obtain limited, one-time use approval of CPNI from a customer during an inbound or outbound call
- The approval lasts **only for the duration of the call**
- The customer's approval does not change the opt-in or opt-out status in any way

CPNI – When You CANNOT Use It

When you receive CPNI from another carrier for provisioning or billing purposes

- Carriers must use CPNI received from other carriers for the purposes of providing telecom service and not for their own marketing efforts
- Carriers cannot use information obtained from another carrier to retain the customer or engage in retention marketing campaigns
- Once a customer has been "lost," however, it is permissible for the carrier to engage in "win-back" campaigns

For anticompetitive purposes such as to identify or track customers that call competitors

CPNI Breach Notifications

A CPNI breach is defined as any instance in which a person, without authorization, has intentionally gained access to, or disclosed customer proprietary information

When a customer's CPNI is breached, the carrier must notify both the customer and law enforcement

Enforcing CPNI Rules

Telecom carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place

All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI

- Carriers shall retain the record for a minimum of one year

Annual Certification of CPNI Compliance

- Newly reinstated requirement!
- Must be filed with the FCC on, or before, March 1st annually
- First reinstated certification due March 1, 2018 (no filing in 2017 required)

Data Security Best Practices

Carriers should voluntarily follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework to provide reasonable measures to protect customer data

https://www.nist.gov/cyberframework/industry-resources

Red Flag Rules

The "Red Flag" rules contain 26 "red flags" that indicate the possibility of Identity Theft

Section 111 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT") Act defines "identity theft" as "a fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade] Commission may prescribe, by regulation

To Whom Do the Rules Apply?

Requires "creditors" to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts

The Federal Credit Reporting Act (FCRA) defines "creditor" to include a person who arranges for the extension, renewal, or continuation of credit, which in some cases could include third-party debt collectors

Additionally, 16 C.F.R. §681.2(b)(5) states that creditors include "…lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies." *(emphasis added)*

Application of Rule Clarified

The Federal Trade Commission (FTC) has determined that even if a company meets the definition of "creditor," it may not be required to comply

- **Ask whether the company regularly and in the ordinary course of business:**
  - Gets or uses consumer reports in connection with a credit transaction
  - Gives information to credit reporting companies in connection with a credit transaction
  - Advances funds to — or for — someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)
- **If you answer:**
  - No to all, the Rule does not apply
  - Yes to one or more, the company must comply

Program Guidelines

Four basic elements must be included in the written Red Flag Program :

- Identify Red Flags
- Detect Red Flags
- Prevent and Mitigate Identity Theft
- Update the Program

Sources

- http://www.businessinsider.com/facebook-beats-privacy-lawsuit-in-us-over-user-tracking-2017-7)
- https://www.nytimes.com/2017/06/23/technology/gmail-ads.html?rref=collection%2Ftimestopic%2FPrivacy&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection
- https://www.nytimes.com/2017/03/29/technology/personaltech/what-the-repeal-of-online-privacy-protections-means-for-you.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=Marginalia&pgtype=article
- https://www.washingtonpost.com/opinions/no-republicans-didnt-just-strip-away-your-internet-privacy-rights/2017/04/04/73e6d500-18ab-11e7-9887-1a5314b56a08_story.html?utm_term=.367f854065bb
- http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/
- http://bgr.com/2017/06/26/att-internet-privacy-charge/

Dee Dee Longenecker
Staff Director – Regulatory Affairs
JSI – Texas Office
dlongenecker@jsitel.com
512-338-0473