Back to School: Data Privacy and Security Basics for Every Businesses

September 11, 2013

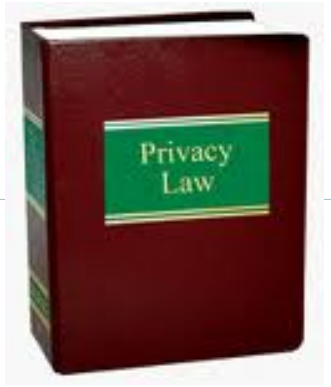
Agenda

- Overview
- Contract Considerations
- Payments & Collections
- Mergers & Acquisitions
- The Cloud
- Mobile Product Development
- Marketing
- Employee Privacy
- When Something Goes Wrong
- Questions

What is "privacy law"?

- Rules regarding the collection and handling of "personal" or "personally identifiable" information (PII)
- AND the notice and choice provided to the consumer about such activities.
- "Data Security" is the related set of practices designed to ensure compliance with requirements that PII and other sensitive information be collected, stored, transmitted and disposed of in a secure manner.

Overview: Privacy Law



No comprehensive privacy law in U.S.

- Generally, the data collector owns and controls the data
- Except in specifically regulated areas, can use data as desired as long as consistent with privacy notices and consent is obtained

Internationally, laws vary

Overview: Sources of General U.S. Privacy Law and Enforcement

- Federal Trade Commission
  - FTC Act
  - Section 5 Enforcement actions
- U.S. Commerce Department
  - Cybersecurity
  - Mobile app transparency
- State laws
  - Data Security
  - California – Mobile apps

Overview: Security/Data Breach Law

- Data disposal/ destruction laws
- Breach notification laws
- FTC applies "reasonableness" standard
- State data security laws
- Sectoral requirements (HIPAA, HITECH, etc.) may be more stringent

Privacy by Design

Basic concept: privacy concerns should be addressed at every stage of product development

Endorsed by FTC in March 2012 report entitled "Protecting Consumers' Privacy in an Era of Rapid Change"

Concept has been included in legislative proposals

Central to policy discussions of privacy in mobile context

FTC enforcement

FTC alleged that HTC America, a mobile device manufacturer, did not build privacy protections into code, putting consumer data at risk and subjecting the company to Section 5 enforcement.

What does this mean for you?

Privacy and data security obligations extend throughout your business:

Contracts with Service Provider

Risks associated with data breaches magnified when your data is outside your control

Due Diligence to be performed:	Where the service provider will store the data (cloud or not)
	What the service provider will do with it (only on your behalf, or independent rights?)
	When you can gain access, or alter the contract
	Who else is touching the data (subcontractors? Independent rights?)
	What happens if there is a breach?
	What happens if there a third party claim?
	Whether to seek indemnity for violations of law?
	Representations and warranties?
	Return of data?

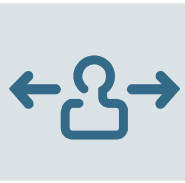
Then Document it…

Privacy and Security Contract Language

Checklist

- ☐ **DEFINE** Confidential Information and Ownership
- ☐ **LIMIT** collection, access, use, disclosure, and retention
- ☐ **ESTABLISH SECURITY STANDARDS** for transmission and storage
- ☐ **OBTAIN** audit rights
- ☐ **OUTLINE** BREACH/INCIDENT RESPONSE

Contracts with Third Parties: Include Data Security Breach/Incident Response



Indemnification

Credit Monitoring

Resolution

Investigation Rights

Insurance Coverage

Notices:

- to Company
- to affected individuals
- to law enforcement

Payments & Collections: Payments

- Payment Card Industry Data Security Standards (PCI DSS)
- Payment Application Data Security Standards (PA-DSS)
- Outsourced for compliance?

Fair Credit Reporting Act Major Issues:

- Are you obtaining a "consumer report"?
- Is there a permissible purpose to obtain and use a consumer report?
- Duties of "furnishers"
- Beware stealth FCRA triggers: Spokeo

Payments & Collections: Credit

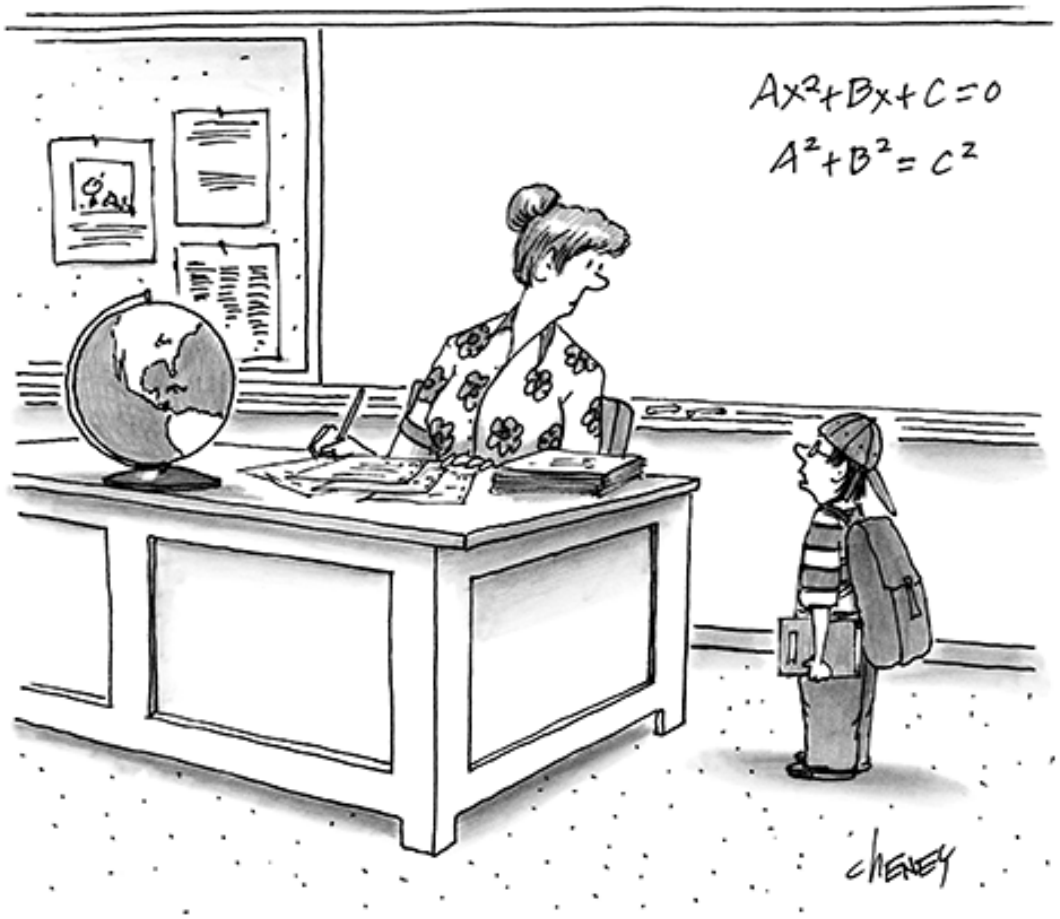
- FCRA adverse action notices: Must give notice to consumer if business takes adverse action based in part on a consumer report from a CRA

- Federal Reserve (now CFPB) has a model adverse action notice for FCRA/Reg. B

Mergers, Acquisitions and Divestitures

- Employee and customer data = biggest asset?
- Consider due diligence on privacy and data security when:
  - Transactions involve personally identifiable assets (customer databases, social media, etc.)
  - Transactions involve data security representations
- Review privacy policies to ensure promises kept

Privacy in the Cloud



"The cloud ate my homework."

IT Solutions – The Cloud

- More data moving to the cloud
- Customers may purchase Software, Infrastructure, Platform – all "as a service"
- Different Types of Cloud Services
  - Private (internal organization)
  - Community (education, health, payment)
  - Public (Amazon, Microsoft, Google)
  - Hybrid
- Unique contract issues
  - Cybersecurity protections
  - Review/audit rights
  - Jurisdictional issues - restrictions in contracts
  - Access rights

Mobile Product Development

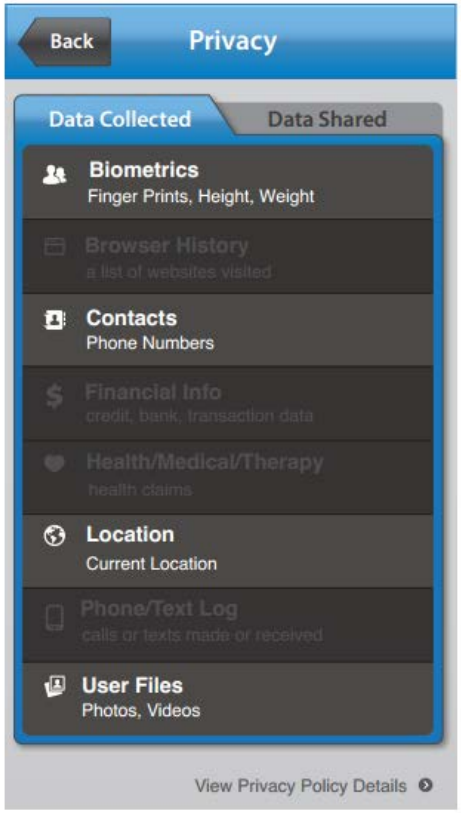
- FTC privacy report, calling for improved mobile disclosures (3/2012)
- FTC workshop on mobile privacy (5/2012)
- FTC guidance on privacy/ad disclosures for mobile apps (9/2012)
- NTIA stakeholder discussions re: mobile apps begin (7/2012)
- California Online Privacy Protection Act (Business and Professions Code section 22575)
  - California AG agreement with Mobile Apps Marketing Companies (2/22/12)
  - California AG letters to 100 companies re: mobile privacy policies (10/30/12)
  - California AG files suit against Delta (12/2012)
- California AG's "Privacy On The Go" Report (1/2013)
- FTC report "Mobile Privacy Disclosures: Building Trust Through Transparency" with recommendations for platform providers, app developers and ad networks and other third parties (2/2013)
- NTIA Multistakeholder Process releases "Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices" and launches consumer testing of short-form notices about the collection and sharing of consumer information with third parties.

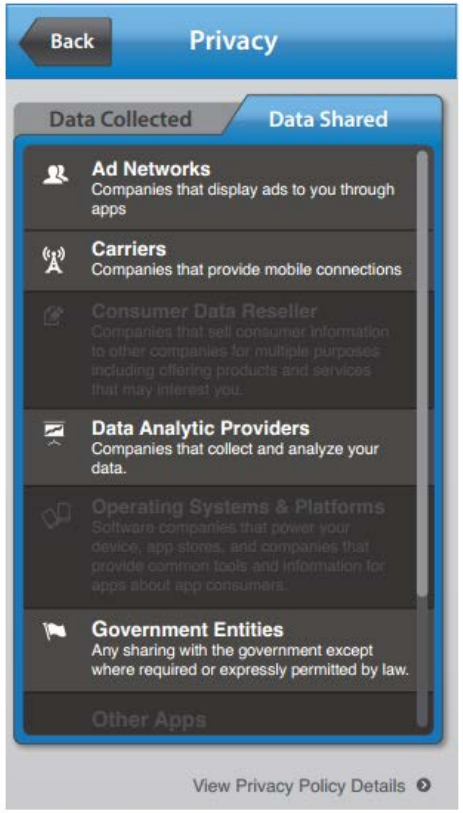
Overview: Mobile Product Development

- Concerns that mobile services and apps violate privacy by collecting and storing information about users' locations
- Challenges of obtaining consent.
- Challenges with communicating disclosures on a small screen.
- NTIA Multi-Stakeholder Process designed to address these issues wby designing a common user interface that quickly informs consumers of information collection and sharing activities.
- Jules Polonetsky, Executive Director of the Future of Privacy Forum has described the results as a "'food label' type approach to a privacy notice [that] will give consumers a standardized way to get key privacy information at a glance and will help consumers better understand how apps collect and share data."
- The following pages contain sample notices shown as examples of implementations of the short notice developed by several of the NTIA stakeholders (source: Future of Privacy Forum, http://www.futureofprivacy.org/2013/07/25/ntia-user-interface-mockups/).

NTIA Mobile Short Notice Example 1

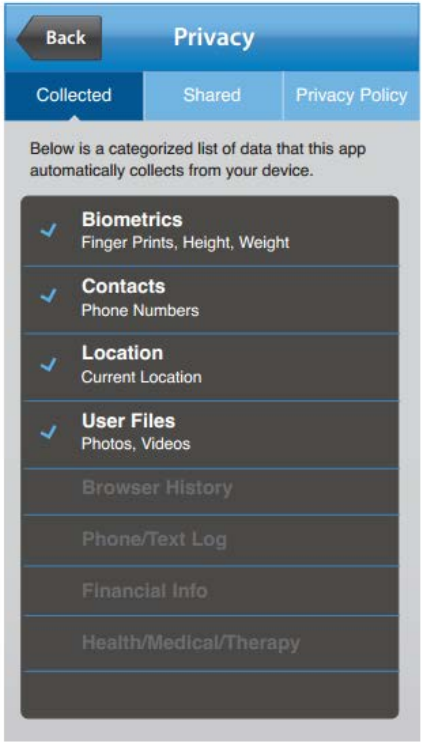
- Data Used Highlighted

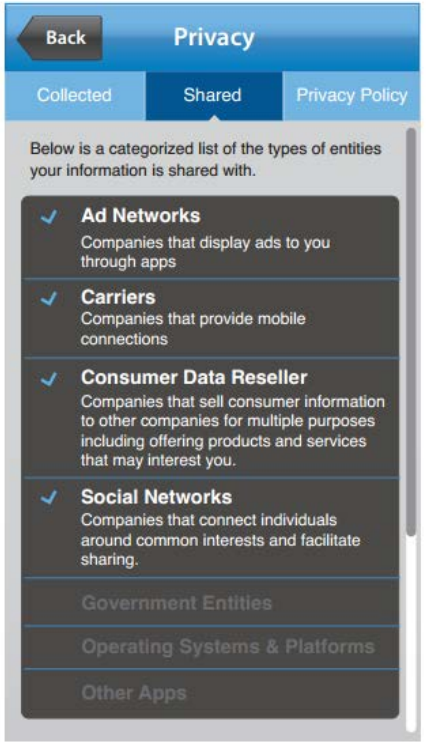




NTIA Mobile Short Notice Example 2

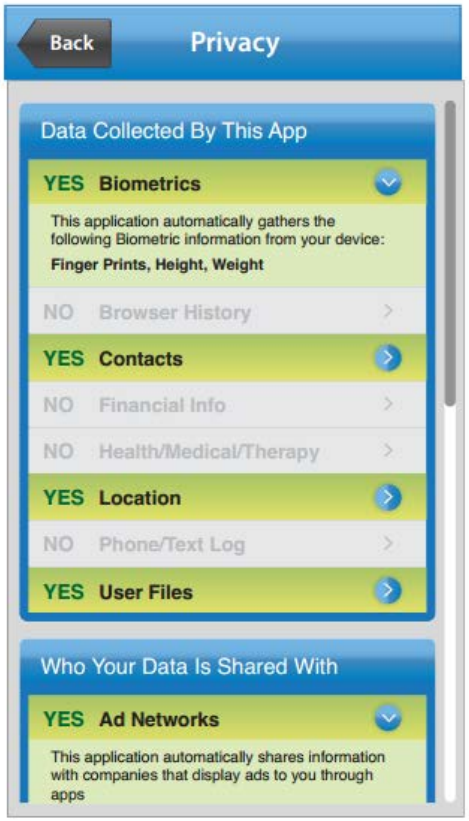
- Data Used on Top and Data Not Used on Bottom

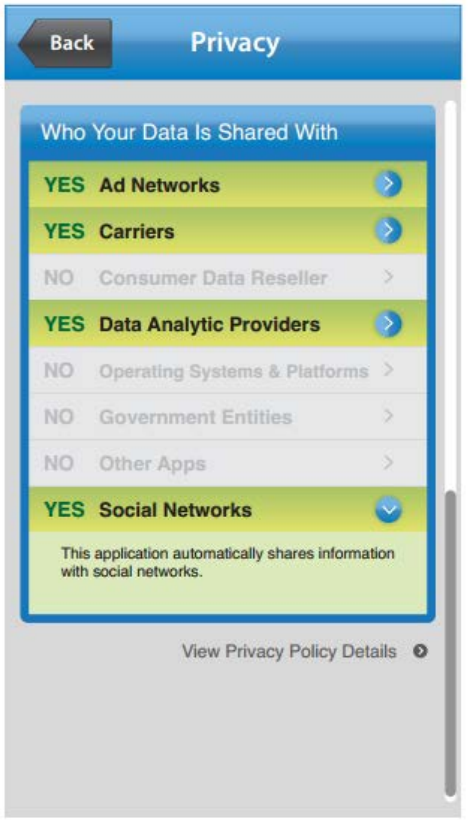




NTIA Mobile Short Notice Example 3

- YES/NO Highlighted Accordion

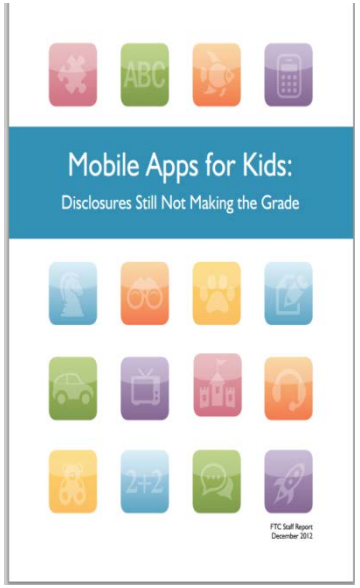




Marketing - children

- The Children's Online Privacy Protection Act ("COPPA") applies to websites directed at children under 13 that collect personal info from them, or general websites that have actual knowledge that they are collecting info from children
- These websites must:
  - Post privacy policy on homepage & link to it where data is collected
  - Obtain verifiable consent from parent before collecting data
  - Offer parental choice regarding use of data, parental access to info & ability to delete
- Modifications to the COPPA rule became final in Dec. 2012. Some highlights include:
  - Geolocation information, photographs, and videos now treated as personal information that cannot be collected without parental notice and consent
  - Closes loophole allowing kid-directed apps/websites to permit third parties to collect personal information through plug-ins (e.g., Facebook plug-ins) without consent
  - Extends COPPA coverage to "persistent identifiers" that can recognize users over time and across different websites or online services, such as IP addresses and mobile device IDs
- **FTC settlement with Artist Arena for $1 million**

Kids + Mobile Apps



- In Dec. 2012, FTC released "Mobile Apps for Kids: Disclosures Still Not Making the Grade"
  - 80% of vendors of apps for kids fail to notify parents about what data they're collecting from kids, how they're sharing it, and who has access to it.
  - Nearly 60% of apps surveyed transmitted user information back to the developer or to an advertising network analytics company or other third party
  - 58% contained advertising within the app, but only 15% indicated the presence of advertising prior to download
  - 22% contained links to social networking services, but only 9% disclosed that fact.
  - 17% allowed kids to make purchases for virtual goods
  - **FTC settlement with W3 Innovations, LLC (d/b/a/ Broken Thumbs Apps) for $50,000**

Marketing – Social Media Challenges

Does Privacy Policy Address Social Media?

FTC Action

Potential Invasion of Privacy Claims

International Issues

Kids

Important to Establish Corporate Policies

Human Resources – Employee Privacy

Pre-employment background checks

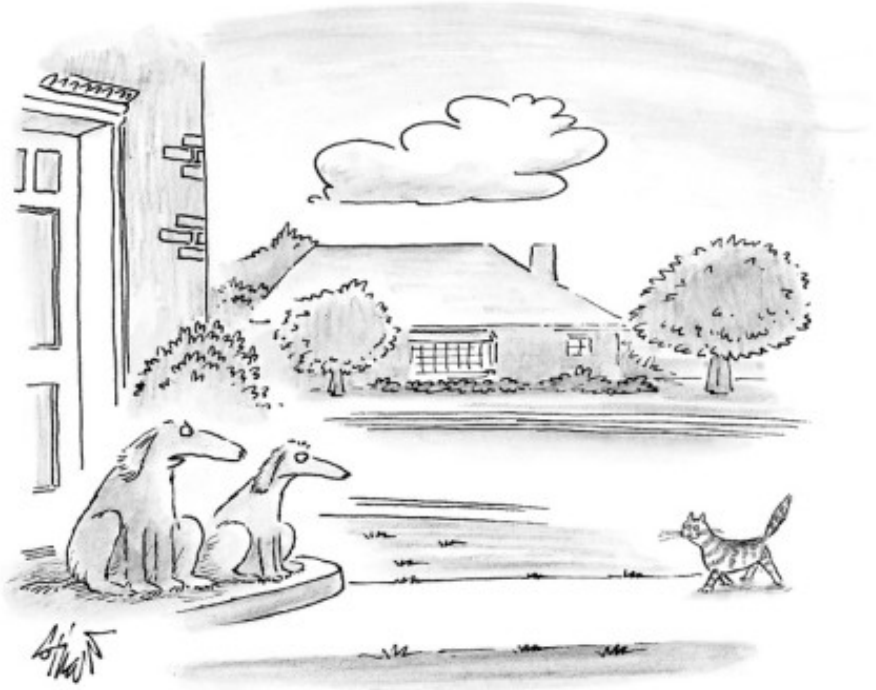
- State laws limit check of criminal history
- FCRA governs check of finances

Bring Your Own Device?

Employee personal use of social media

State legislation passwords/login

What do you do when something goes wrong?



"There's obviously been a serious breach of security."

Breach Response Plan

- Have a plan in place before the breach occurs!
- Create a security breach response team that includes legal, IT, security, HR, and media relations functions
- Train employees in implementing the plan
- Test response plan

State Data Breach Notification Laws

46 states and District of Columbia (no AL, KY, NM, SD)

Most apply to electronic information (vs. physical document)

Often define personal information as: An individual's first name or first initial and last name plus one or more of following data elements:	(i) Social Security number,
	(ii) driver's license number or state-issued ID card number,
	(iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account.

But Beware of North Dakota and recent trend for broader definition of PI

Frequent requirement to report to state official/AG, credit reporting bureaus

Risks associated with a data breach

Legal action by regulatory agencies, law enforcement and/or private litigants	Federal Trade Commission
	State AGs and Congressional Inquiries
	Class Action Litigation
EU, Canadian or other foreign govt enforcement	
Reputational Harm	

FTC Enforcement

FTC: increased enforcement activities and testing limits of Section 5 Authority http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml:

- **Google Buzz**(March 2011): Gmail users who opted out of Buzz were nonetheless enrolled; users were not adequately informed that the identity of individuals they emailed most frequently would be made public by default, and users who clicked "Turn Off Buzz" were not fully removed from the social network.
- **Facebook** (Nov. 2011): changed privacy settings without notice or consent; made data public that users had designated as private
- **RockYou** (Mar. 2012): failed to implement reasonable security procedures to protect users' data; violated COPPA by collecting & disclosing children's info without parental consent
- **MySpace** (May 2012): violated own privacy policy by sharing personal information with advertisers; allowed targeted ads without notice.
- **Wyndham Hotels** (June 2012): FTC sued for failure to protect consumer info from three data breaches. **Wyndham has filed MTD, alleging that FTC has no authority to decide whether data protection policies are "unfair," "reasonable," or "appropriate."**
- **Google Cookies** (August 2012): agreed to pay a record $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating the earlier Google Buzz settlement with the FTC.
- **Path** (Jan. 2013): improperly collected info from consumers' mobile device address books, collected kids' data without parental consent.

Litigation Trends

- Most common result: privacy lawsuits end at the Motion to Dismiss stage – no harm or standing
- Some recent cases: more lenient on "harm" standard where statute creates right of action, damages (e.g. Jewel v NSA (surveillance) & Edwards v First American Corp. (RESPA))
- Even an unsuccessful privacy class action suit can conceivably cost a defendant millions of dollars.
- Arbitration clauses

Federal Statututes with Statutory Damages and Private Rights of Action

- Computer Fraud and Abuse Act, 18 U.S.C. § 1030
- Electronic Communications Privacy Act (ECPA), including
  - Wiretap Act, 18 U.S.C. §§ 2510-2522
  - Stored Communications Act, 18 U.S.C. §§ 2701-2712
  - Video Privacy Protection Act, 18 U.S.C. § 2710
- Telephone Consumer Protection Act, 47 U.S.C. § 227
- Fair Credit Reporting Act, 15 U.S.C. § 1681
- Cable Act, 47 U.S.C. § 551
- Satellite Home Viewer Extension and Reauthorization Act, 47 U.S.C. § 338(i)

Thank You!

Questions?

Bob Scott
Washington, DC 20006
(202) 973-4265
BobScott@dwt.com

Christin McMeley
Washington, DC 20006
(202) 973-4264
ChristinMcMeley@dwt.com