Richard C. Hsu
Shearman & Sterling
rhsu@shearman.com

# CIPP/US Privacy Summary*

## Federal

## Healthcare

### HIPAA

- Applies to "Covered Entities"
  - Healthcare Providers
  - Healthcare Insurers
  - Healthcare Clearinghouse
  - Does not include medical websites, etc.
- Applies to all forms (oral, paper) of Protected Health Information (**PHI** including **IIHI**)
- Enforcement by Dept of HHS / FTC
- No State PreEmption
- No private right of action

### HIPAA

- **HIPAA Privacy Rule**
  - Must provide Privacy Notice and get consent at the time of service
  - Covered Entities may only use "Minimum Necessary" **PHI** for Treatment, Payment and Operations (**TPO**); otherwise must *Opt-In*
- **HIPAA Security Rule**
  - Only covers ePHI and establishes min requirements for ePHI
  - Confidentiality Integrity Availability (**CIA**)

### HITECH

- Expands HIPAA as use of ePHI grows
- Expanded HIPAA to include "Business Associates"
- Notification requirements for breach of un-encrypted data to consumer/HHS/FTC

### GINA

- No discrim based on genetic info
- Cannot require EE to take genetic test

## Telecomm

### TSR
### Do Not Call Registry

- Consumer can elect to be on DNC list for telemarketing calls
- Does not apply to political calls, **EBR**, non-profits calling on their own
- **DNC** Safe Harbor for inadvertent mistake
- Rules for Call Abandonment (3%)
- Must *Opt-In* for Robocalls (Rx calls ok)
- No State PreEmption

### CAN-SPAM

- Designed to give consumer right to *Opt-Out*
- No false or misleading headers
- **MSCMs**
  - Applies to phone-to-phone
  - Must *Opt-In*
  - FCC maintains registry of domains
- Enforcement by FTC / FCC
- State PreEmption (for the most part)

### Other

- Telecomm Act
  - Applies to telecomm carriers; not Internet
  - Can only use **CPNI** internally (o/w must *Opt-In*)
- Cable TV Privacy Act
  - Regulates disclosure of **PI**
- Video Privacy Protection Act (**VPPA**)
  - Private right of action
  - Does it apply to streaming video?

## Financial

### FCRA

- Regulates CRAs incl. Equifax, Transunion and Experian
- CRA = "consumer" not "credit"
- "Users" must have "Permissible Purpose" to obtain CRAs
- Requires Privacy Notice and *Opt-In*
- Must provide consumers "Access" and notice of "Adverse Actions"
- Enforcement by FTC / CFPB

### FACTA

- Expands FCRA to any credit tx
- Requires trun-cation of CC/DC #
- Must provide free annual CRs
- CRAs must allow *Opt-Out*
- **Disposal Rule**
  - Must dispose after use
- **Red Flags Rule**
  - Mitigate and detect identity theft
  - 2010 narrowed def of creditor

### GLBA

- Applies to all domestic FI's and non-public **PI**
- **GLBA Privacy Rule**
  - Must provide clear and conspicuous Privacy Notice
  - Right to *Opt-Out* (with exceptions)
- **GLBA Safeguards Rule**
  - Comprehensive Security Program
  - Administrative, Technical, Physical Security
  - Safeguards must be "appropriate" to size and scope

### Dodd Frank

- Created **CFPB** for enforcement
- Addresses "Abusive Acts and Practices" which take advantage of consumer's lack of understanding

### AML

- Bank Secrecy Act
  - Report any tx >$10k
- "Follow the Money"
- Suspicious Activity Report (**SAR**)
- USA Patriot Act

## Children

### COPPA

- Applies to websites
  - (a) aimed at or
  - (b) which collect PI from

  children *under the age of 13*
- Must post privacy notice on homepage
- Must obtain verifiable parental consent by postal mail (*Opt-In+*)
- Several exceptions to parental consent and Safe Harbor for compliance w/FTC approved group
- Enforcement by FTC
- State PreEmption

## Education

### FERPA

- Only applies to institutions which receive Fed Funds
- Applies to Educational Records
- Must provide students "Access" w/in 45 days
- May file complaint with Dept of Ed. but no private right of action

### PPRA

- Expanded to parents of minors
- Applies to secondary schools that receive Fed Funds

### NCLB

- No Child Left Behind

*Adapted from IAPP CIPP/US Privacy Certification

Richard C. Hsu
Shearman & Sterling
rhsu@shearman.com

# CIPP/US Privacy Summary*

## Regulators

### FTC

- **Section 5**: No "unfair or deceptive acts or practices"
- Enforcement Agency for
  - **COPPA**
  - **CAN-SPAM** (w/FCC)
  - **HIPPA** (w/HHS)
  - **FCRA/FACTA/GLBA** (w/CFPB)
- Most enforcement actions are settled through Consent Decrees (which are made public)

### "Unfair"

- ***Eli Lilly***
  - Eli Lilly accidentally sent email addresses to 600+ individuals
  - "Unfair" b/c they failed to implement reasonable security program
- ***BJ's Wholesale Club***
  - Failure to encrypt PI was "unfair trade practice"
  - Nothing deceptive

### "Unfair and Deceptive"

- ***Gateway Learning***
  - Retroactive changing of privacy policy was "unfair trade practice" even if accurate
- ***In Re Google Buzz***
  - Failure to follow its own privacy policy was "deceptive trade practice"
  - First US-EU Safe Harbor enforcement by FTC

### Self-Regulation

- **PCI-DSS** (credit card)
- Digital Advertising Alliance (**DAA**)
- TrustMarks
  - Verisign, BBB, TRUSTe

### Cross-Border

- US-EU Privacy Shield (for US only)
  - Formerly Safe Harbor
  - Enforced by Dept of Commerce
- **BCR** (Binding Corporate Rules)
- Model Contracts
- Consent of the Data Subject

### Int'l Regs

- **GDPR**
  - General Data Protection Regulation (EU Data Protection Directive)
- **GPEN**
  - Global Privacy Enforcement Network
- **APEC**
  - Asia-Pacific Economic Cooperation
  - **CPEA** (Cross-Border Privacy Enforcement Arrangement)

## Workplace

### Background Screening

#### FCRA

- May be used to perform credit and background checks
- Must obtain written notice and consent (*Opt-In*)
- **ICRAA**
  - California law for investigations
  - Disclosure requirements and consent are stricter

#### ADA

- Before offer, Company may require medical exam only where job related
- After offer, Company may require medical exam if consistent
- Prohibits question about prior injuries or illness
- Psychological test are largely prohibited as being "medical exams"

### During Employment

#### EPPA

- Employee Polygraph Protection Act prohibits use of lie detectors
- Exceptions for jobs which involve security or drugs
- Employers must post **EPPA** provisions in conspicuous location
- No State Law PreEmption
- Private Right of Action

#### Drug Testing / Monitoring

- Drug Testing generally allowed (*not* considered medical exam under **ADA**)
- Video Surveillance / Monitor
  - No federal law, but states have limits (eg CA, MI) + tort actions
- Telephone calls and emails are generally protected (**ECPA**)
- Stored Communications (**SCA**)

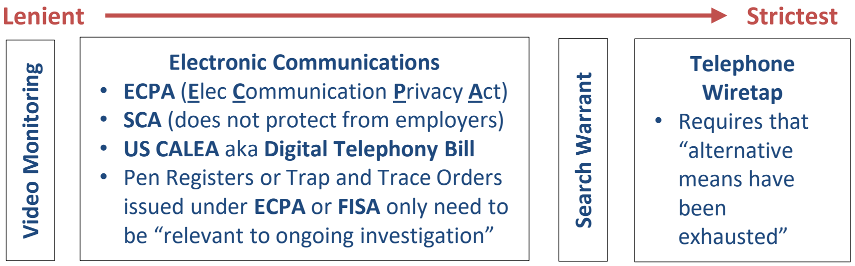
## Government Access

### Financial

- **RFPA** (Right to Financial Privacy Act)
- No gov't may have access to financial records unless "reasonably described" + 1 other condition is met

### Media

- **PPA** (Privacy Protection Act)
- Passed in response to *Zurcher v. Stanford*



Lenient → Strictest

Video Monitoring

#### Electronic Communications

- **ECPA** (Elec Communication Privacy Act)
- **SCA** (does not protect from employers)
- **US CALEA** aka **Digital Telephony Bill**
- Pen Registers or Trap and Trace Orders issued under **ECPA** or **FISA** only need to be "relevant to ongoing investigation"

Search Warrant

#### Telephone Wiretap

- Requires that "alternative means have been exhausted"

### National Security

- **FISA** (Foreign Intelligence Surveillance Act)
- USA Patriot Act
- **NSL** (National Security Letters)
  - May be issued w/out judicial authorization

*Adapted from IAPP CIPP/US Privacy Certification