

Privacy Boot Camp: A Pragmatic Approach to Surviving the Regulatory Wilderness

Please pull up <https://kahoot.it/> on your device

Presented by:

Kathleen Sutherland
Deborah O'Connor
Holly Benton

SCCE Higher Education Compliance Conference
June 2018 (Session P1)



University of Colorado
Boilerplate text about the University of Colorado

Duke OFFICE of
AUDIT, RISK & COMPLIANCE

students mission financial aid
retention outcomes
HIGHER EDUCATION
Faculty revenue tuition online regulation
State Authorization degree diversity admissions

- Management and operations are decentralized
- Resources are limited
- Governance is shared
- Academic freedom is a core value



University of Colorado
Boilerplate text about the University of Colorado

Duke OFFICE of
AUDIT, RISK & COMPLIANCE

students mission financial aid
retention outcomes
HIGHER EDUCATION
Faculty revenue tuition online regulation
State Authorization degree diversity admissions

- Complex compliance requirements cut across functional areas (silos)
- Regulations intended for other industries impact higher ed ops in ways never contemplated
 - Banking / Financial Services
 - IT / Telecomm
 - Healthcare



University of Colorado
Boilerplate text about the University of Colorado

Duke OFFICE of
AUDIT, RISK & COMPLIANCE

START WHERE YOU ARE
USE WHAT YOU HAVE.
DO WHAT YOU CAN.

- ARTHUR ASHE


- YINHS YZHI

University of Colorado

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

SHARED LANGUAGE




University of Colorado

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

Google Books Ngram Viewer



University of Colorado

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

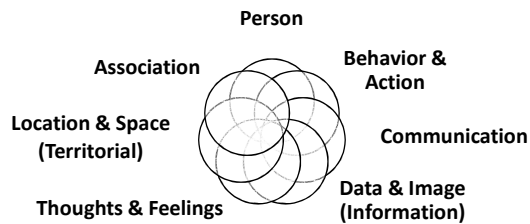
2

PRIVACY

- Broad conceptual definition
 - “Right to be let alone”
 - Warren & Brandeis 1890 law review article
 - Freedom from interference or intrusion
 - State or condition of being free from being observed or disturbed by other people



MULTIPLE DIMENSIONS OF PRIVACY



DATA & IMAGE

- Protection of personal info in all forms
 - Data, printed info, images
- Activity focuses on establishing rules that govern collection, use, sharing and handling of personal information
 - Financial info (bank & credit card accounts)
 - Medical info (provider & insurance records)
 - Government records (SSN)
 - Online activity (through access logs, tracking)
 - Photos & videos taken / shared without consent
 - Biometric / genetic data

“PERSONAL INFORMATION”

- Not all definitions are equivalent (especially for legal purposes)
 - Personally identifiable information (PII)
 - Sensitive personal information (SPI)
 - Personal data / “Special” data categories (EU regime)
- Generally, “PII” (in US context) is info that:
 - Can be used on its own or with other information to
 - Identify, contact, or locate a single person, or to
 - Identify an individual in context



DEFINITIONS MATTER!

“Personal Data” (GDPR Article 4(1))

- “Any information **relating** to an identified or **identifiable** natural person (“data subject”)”



“Personal Information” (CRS § 6-1-716)

- “a Colorado resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are **not encrypted, redacted, or secured by any other method** rendering the name or the element unreadable or unusable: (A) Social security number; (B) Driver’s license number or identification card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password”
- **Does not include** publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

DEFINITIONS MATTER!

“Special Categories” of Personal Data (GDPR Article 9(1))

- Personal data that reveals “**racial** or **ethnic** origin, **political** opinions, **religious** or **philosophical** beliefs, or **trade union** membership, . . . **genetic** data, **biometric** data for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a natural person’s **sex life** or **sexual orientation**”

“Sensitive” Personal Information (FTC 2012 Report)

- “The Commission defines as sensitive, **at a minimum**, data about children, financial and health information, Social Security numbers, and certain geolocation data”

PRIVACY / SECURITY

- Privacy
 - Focus on the use and governance of personal data and norms around surveillance /observation
 - Policies and practices to ensure that personal information is being collected, shared and used in appropriate ways
- Security
 - Focus more on protecting data and IT systems from malicious attacks and the exploitation of stolen data



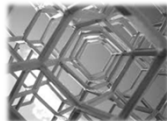
COMPLIANCE CHALLENGE

- Three approaches to info privacy regulation globally:
 - United States: Sector-specific and data-specific
 - European Union: Omnibus privacy laws applicable to all PII, regardless of sector, category of individual, or type of PII
 - Rest of World: Mix of US and EU approaches



“FAIR INFORMATION PRACTICE PRINCIPLES”

- Blend of substantive and procedural principles to be used in evaluation and consideration of systems, processes, or programs that affect individual privacy
- Basis of a number of privacy frameworks and standards
- Building blocks of modern information privacy law





PRIVACY FRAMEWORKS

- Fair Information Practice Principles (FIPPs)
 - US Dept. Health, Education, and Welfare 1973 Report (Privacy Act of 1974)
- Generally Accepted Privacy Principles (GAPP)
 - AICPA/CICA (business/management perspective on privacy obligations, risks & opportunities)
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
 - Organisation for Economic Cooperation and Development (OECD, 1980/2013)



PRIVACY FRAMEWORKS

- APEC Privacy Framework
 - Asia-Pacific Economic Cooperation Electronic Commerce Steering Group (ECSG 2005)
- Security and Privacy Controls for Federal Information Systems and Organizations
 - NIST SP 800-53 (Rev. 4); "Privacy Control Catalog" (2015)
- ISO/IEC 29100: 2011 – Information technology – Security techniques – Privacy framework



TRANSPARENCY

Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).



INDIVIDUAL PARTICIPATION

Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII.

Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.



PURPOSE SPECIFICATION

Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.



DATA MINIMIZATION

Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).



USE LIMITATION

Organizations should use PII solely for the purpose(s) specified in the notice.

Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.



University of Colorado
Boulder | Colorado Springs | Fort Collins | Denver | Anschutz Medical Campus

Duke | OFFICE of
AUDIT, RISK & COMPLIANCE



DATA QUALITY AND INTEGRITY

Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.



University of Colorado
Boulder | Colorado Springs | Fort Collins | Denver | Anschutz Medical Campus

Duke | OFFICE of
AUDIT, RISK & COMPLIANCE



SECURITY

Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.



University of Colorado
Boulder | Colorado Springs | Fort Collins | Denver | Anschutz Medical Campus

Duke | OFFICE of
AUDIT, RISK & COMPLIANCE



ACCOUNTABILITY AND AUDITING

Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

PRINCIPLES OF PRIVACY BY DESIGN (PbD)

- Proactive not reactive, preventive not remedial
- Privacy as the default setting
- Privacy embedded into the design
- Full functionality: positive sum, not zero sum
- End-to-end security: full lifecycle protection
- Visibility and transparency: keep it open
- Respect for user privacy: keep it user-centric



Privacy
baked in

<https://www.rverson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design>



PRIVACY PROGRAM


- "Privacy" and privacy risks properly defined and identified?
- Responsibility and accountability for managing privacy program assigned?
- Understand gaps in privacy management?
- Monitor privacy management?
- Train and/or educate students, faculty and staff?
- Incident response plan?
- Communicate privacy-related matters and update communications as needed?



Operationalizing Privacy: A Pragmatic Approach

Pragmatic: "Dealing with things sensibly and realistically in a way that is *based on practical* rather than theoretical considerations."





University of Colorado


Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

START WHERE YOU ARE.
USE WHAT YOU HAVE.
DO WHAT YOU CAN.

- ARTHUR ASHE

- VINOD KUMAR




University of Colorado


Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

FUNDAMENTAL STEPS

- Know your basis of support
- Ensure a seat at the table
- Get a legacy check-in
- Assess your culture for privacy awareness
- Understand the appetite for risk
- Identify champions
- Manage expectations!





University of Colorado

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

10

GET A HANDLE ON YOUR UNIVERSE!



- Scope your role
- Identify your partners
- Discern data governance
- Map your landscape
- Foster awareness

WHAT'S YOUR SCOPE?

- Operational Program Owner
 - Policy owner/enforcer
 - Incident management
 - Vendor/contract review
 - Monitoring
- Strategic Partner
 - Consultant
 - Assessments
 - Shared Risk Owner



- Subject Matter Resource
- Assurance Provider
 - Compliance reviews; audits
- Other
 - HIPAA Privacy Officer
 - GDPR Data Protection Officer

IDENTIFY KEY PARTNERS

- | | |
|--------------------------|---------------------|
| • Data Stewards | • Student Affairs |
| • Compliance Risk Owners | • Human Resources |
| • Information Security | • Libraries |
| • IT | • Records Retention |
| • Legal | • Risk Management |
| • Compliance | • Health System CPO |
| • Audit | • Athletics |
| • IRB | • Students |
| • Registrar | • Faculty |
| • Financial Aid | • Staff |



It's all about relationships...



- Leadership/Governance committees
- Privacy Liaisons and/or committees
 - Departments, Schools, Institutes
 - Stakeholder groups
 - Partner groups
 - IRB/Contracts/Security
 - HIPAA impacted
 - GDPR impacted

YOUR OCEAN . . . Data Governance Questions



- Who?
 - Who is in charge?
 - Who are the stakeholders?
 - Who are your resources?
- What/Why?
 - What information? Why?
 - What are the musts to you? Why?
 - What's your role?
 - What are others' top issues? Why?
- Where?
 - Where are your greatest risks?
 - Where are the impacts?
 - Where is your scope within those?
- When?
 - When do you address?
 - When do you escalate?
 - (And to whom/what body?)

MAP YOUR LANDSCAPE



- Risk Assessment
- Data Mapping
- Identify past efforts
 - Audits
 - IT Security Reviews
 - Compliance Reviews
- Privacy Impact Assessments/DPIAs

GO FOR THE “AHA!” MOMENT

- Communicate/Message/Brand
 - Available Forums, Media
 - Roadshows/Campaigns
 - Swag!
- Ground the Message
 - FIPPs; PbD – bake it in!
 - Information Asset Lifecycle Management
- Promote the “Golden Rule of Privacy”

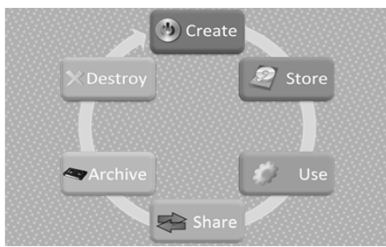


“FIPPs”

- Notice/Awareness
- Choice/Consent
- Collection Limitation
- Access/Participation
- Integrity/Security
- Accountability

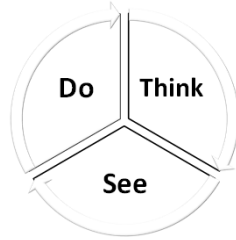


INFORMATION ASSET LIFECYCLE



The *Golden Rule* of Privacy:

Think-See-Do!



The EU GDPR@ Duke: A Great “Opportunity”

- Scope
 - Measured approach
- Partners
 - Enterprise
 - Identity Management
 - Research partners
 - Impacted Areas
 - Identify leadership
 - Identify Point People
- Governance
 - Three tier
- Landscape
 - Document Article 30
- Awareness
 - Impacted Areas
 - Enterprise-wide



Privacy “Hot Spots”: What’s on Your Risk Radar?



Please pull up <https://www.polleverywhere.com>

Focus discussion on topics most relevant to you . . .



PRIVACY “HOT SPOTS”

- HIPAA
- GLBA / Red Flags
- Internet of Things (IoT)
- GDPR / International Law
- Big Data / Research / Vendor Management
- Recording / Surveillance
- State Breach / Open Records Laws



ARCHIVE OR DESTROY?

- Data archiving:
 - Process of moving data that is no longer actively used to a separate storage device for long-term retention
- Archive data:
 - Older data that is still important to the organization, needed for future reference
 - Data that must be retained for regulatory compliance



WIPING DATA



START WHERE YOU ARE.
USE WHAT YOU HAVE.
DO WHAT YOU CAN.

- ARTHUR ASHE

University of Colorado
UNIVERSITY OF COLORADO

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

HIPAA REVISITED

- *When was the last time you reviewed . . . ?*
 - HIPAA Privacy and Security Policies & Procedures
 - Hybrid Entity Designation
 - Notice of Privacy Practices
 - Business Associate Agreements
 - Security Risk Assessment

University of Colorado
UNIVERSITY OF COLORADO

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

HIPAA ENFORCEMENT TRENDS

OCR has significantly increased focus on HIPAA enforcement in recent years

- Compare these HIPAA fine totals by year:
 - 2015: \$6,193,000
 - 2016: \$23,504,800
 - 2017: \$19,393,200

University of Colorado
UNIVERSITY OF COLORADO

Duke

OFFICE of
AUDIT, RISK & COMPLIANCE

2017 OCR HIPAA Enforcement Fines & Penalties

Organization	Fine Total	Link to OCR Settlement
Providence Health	\$275,000	Link to OCR Settlement
MAFFHC	\$1,200,000	Link to OCR Settlement
Children's Medical Center of Dallas	\$1,200,000	Link to OCR Settlement
Memorial Healthcare System	\$1,500,000	Link to OCR Settlement
Metrix Community Provider Network	\$380,000	Link to OCR Settlement
Center for Children's Digestive Health	\$15,000	Link to OCR Settlement
Cardiacare	\$1,000,000	Link to OCR Settlement
Memorial Healthcare System	\$1,400,000	Link to OCR Settlement
St. Luke's Rosemead Hospital System	\$187,200	Link to OCR Settlement
21st Century Oncology	\$1,200,000	Link to OCR Settlement
2017 Total	\$10,394,200	



Duke OFFICE of
AUDIT, RISK & COMPLIANCE



PREVENTIVE TIPS

- HIPAA Walk Through
 - Watch for "low tech" potential breaches
- Risk Assessment
 - Use published OCR audit programs to support risk assessment
- Privacy Board
- Entrepreneurial "Pop Up" Clinics
- PR / Media Relations / Social Media
- Plan for Interaction with Law Enforcement



Duke OFFICE of
AUDIT, RISK & COMPLIANCE



GLBA REVISITED

- Applies to "financial institutions" handling of customers' "nonpublic personal information"
- FERPA compliance is deemed GLBA Privacy Rule compliance
- Safeguards Rule (16 CFR §314) requires **written information security program** that addresses specific elements
 - Designation of responsible employee, comprehensive risk assessment, implementing safeguards (with testing/monitoring), selection & oversight of 3rd party providers, program evaluations/adjustment
- Original Safeguards Rule compliance required in May 2003
 - Higher Ed – FTC regulatory authority
 - FSA added Program Participation Agreement (PPA) GLBA requirement 2015



Duke OFFICE of
AUDIT, RISK & COMPLIANCE

GLBA

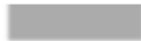
- Dept. Ed “Dear Colleague Letters” re protecting student info
 - DCL GEN 15-18 & GEN 16-12: Student financial aid info subject to GLBA Safeguards Rule
 - “Strongly encourages” institutions to review and understand NIST SP800-171 standards for protecting Controlled Unclassified Information (CUI)
 - Contractual obligation to protect data under FSA PPA and SAIG Enrollment Agreement
- **GLBA will (almost certainly) be included in FY19 federal single audit**
 - OMB draft audit objective language released August 2017



GLBA (DRAFT) AUDIT OBJECTIVE

Determine whether the IHE [institution of higher education] **designated an individual** to coordinate the information security program; **performed a risk assessment** that addresses the three areas noted in 16 CFR 314.4(b) and **documented safeguards** for identified risks.

Federal
Student
Aid



“SUGGESTED AUDIT PROCEDURES”

- Verify that the IHE has **designated an individual** to coordinate the information security program.
- Obtain the IHE risk assessment** and verify that it addresses the three required areas noted in 16 CFR 314.4 (b).
- Obtain the documentation created by the IHE that aligns each safeguard with each risk identified** from step b above, verifying that the IHE has identified a safeguard for each risk.



RED FLAGS RULE



- Fair and Accurate Credit Transaction Act of 2003 (FACTA)
 - FTC to issue regs requiring “creditors” to adopt policies/procedures to prevent ID theft
- Red Flags Rule issued by FTC 2007 (16 CFR § 681.1)
 - “Financial institutions” and “creditors” holding “covered accounts” must develop a written identity theft prevention program designed to identify, detect & respond to “red flags”
 - Amended in 2010 limiting circumstances in which creditors are covered
 - Compliance deadline: December 31, 2010

INTERNET OF THINGS

- Over half the world's internet traffic is not coming from humans
 - Imperva Incapsula Report
- IoT set to overtake mobile phones as largest category of connected devices in 2018
 - Ericsson Mobility Report June 2017
- Gartner forecast: 20.4 billion connected “things” by 2020 (up from 8.4 billion in 2017)
- IoT devices predicted to generate 400 zettabytes (a trillion gigabytes) of data per year in 2018



INTERNET OF THINGS

- How is your institution assessing risk and controlling impact of IoT to computing systems, networks and data?
 - Policies, standards, guidelines addressing adoption of IoT functionality?
 - Risks distinct from traditional computing environment
 - Controls for detecting, evaluating, monitoring, managing introduction of connected devices?
 - Purchasing controls, vendor checklists, training & awareness
- Proactive consideration of privacy impacts / risks due to “out-of-the-box” configuration and weak security controls?
 - Devices collect, transmit and store confidential/personal data




EU GENERAL DATA PROTECTION REGULATION




- Designed to provide EU data subjects more control over their personal data and codifies privacy as a fundamental right
- Applies to organizations with operations in the EU and/or that offer goods or services to and/or monitor people in the EU
- Requires that controllers and processors document the legal basis to transfer and process personal data
- Has extra-territorial reach and imposes significant fines for non-compliance


University of Colorado
Boulder | Colorado Springs | Fort Collins | Denver | Anschutz Medical Campus


Duke | OFFICE of
AUDIT, RISK & COMPLIANCE

EU GENERAL DATA PROTECTION REGULATION



- Protects info of data subjects (natural persons), regardless of nationality
 - Not a “citizenship-dependent” law
- For US academic institutions, “natural persons” will be:
 - Students (going to study abroad programs in the EU)
 - Faculty (hired locally or posted to the EU)
 - Staff and other personnel (hired locally or posted to the EU)
 - Third parties (e.g., EU contractors, donors, researchers)


University of Colorado
Boulder | Colorado Springs | Fort Collins | Denver | Anschutz Medical Campus


Duke | OFFICE of
AUDIT, RISK & COMPLIANCE


PROCESSING OF PERSONAL DATA: PRINCIPLES

ARTICLE 5 - Organization collecting, processing & storing personal data must respect these principles:

- Lawfulness, Fairness & Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity & Confidentiality
- Accountability



University of Colorado
Boulder | Colorado Springs | Fort Collins | Denver | Anschutz Medical Campus

Duke | OFFICE of
AUDIT, RISK & COMPLIANCE

RIGHTS OF DATA SUBJECT

- Full and transparent information and communication
- Right of access
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not to be subject to automated individual decision-making, including profiling



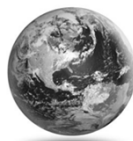
GDPR MYTHS BUSTED

- It applies to everyone!
- Processing of personal data always requires the data subject's consent
- Data Privacy Impact Assessments (DPIA) are mandatory
- You must delete all personal info in response to a "right to be forgotten" request
- You must have a Data Protection Officer (DPO)
- Fines are set: 4% or 20 million Euro, whichever is greater



INTERNATIONAL

- Data privacy laws **other than** GDPR
- Consider impact on:
 - HR operations / Tax obligations
 - Research abroad
 - International investigations (e.g., Title IX study abroad)
 - Export control
 - VPN access / transborder data flow
 - Tech control plan
 - Online ed initiatives
 - Citizenship



EVOLVING GLOBAL LANDSCAPE: ISRAEL



Privacy Protection Regulations (Data Security) 5777-2017 (March 2017)

- Impose mandatory comprehensive data security and breach notification requirements on anyone who owns, manages or maintains a database containing personal data in Israel
 - Resource: <https://iapp.org/news/a/israel-enacts-landmark-data-security-notification-regulations/>

EVOLVING GLOBAL LANDSCAPE: CHINA



- Cybersecurity Law became effective June 2017
- Reforms data management and internet usage regulations
- Imposes specific requirements for network and system security for network operators and businesses in defined critical sectors
- Law has raised concerns among some foreign companies over the greater data controls and increased risk of intellectual property theft

EVOLVING GLOBAL LANDSCAPE: CANADA



- Personal Information Protection and Electronic Documents Act ("PIPEDA") is the federal privacy law applicable to the private sector
- 28 federal, provincial and territorial privacy statutes govern the protection of personal information in the private, public and health sectors
- These statutes vary but set out a comprehensive regime for collection, use and disclosure of personal information



BIG DATA

- Increased connectivity and growth of IoT allows improved analysis
 - Tracking behavior, enhanced situational awareness, operational decision analytics, “personalized” medicine
- Challenges on campus:
 - Data mining for research (secondary uses of data)
 - Large health-related data repositories, biometrics
 - Learning analytics / third party learning tool interoperability apps (LTIs) platforms)
 - “Student success” monitoring platforms (“profiling” perception)
 - Student-focused apps that track, swipe access / banking cards



RESEARCH-RELATED CONCERNS

- Use of data collected from/about students for secondary uses, including research
- Capture, use, further disclosure for research of biometric data
 - State biometric privacy laws, breach laws with biometrics amendments
- “Controlled Unclassified Information” (CUI) – NIST SP 800-171
 - Data that should be safeguarded that is not classified
 - Categories with privacy implications: Research data, student records & PII
- Privacy/security concerns about research apps
- Use of PHI for research, especially research conducted outside CE



VENDOR MANAGEMENT

- Privacy & security control assessment in procurement process
 - Shifting of systems to the “Cloud”
- Appropriate contract language, including data definitions (PII, SPI), encryption & audit provisions
 - Consider requiring Service Organization Control (SOC) Report, third party certification
- Ongoing monitoring & relationship management
- Consideration of data lifecycle & coordinated incident response
- Subcontract considerations (data services “supply chain”)



RECORDING / SURVEILLANCE

- Cameras
 - Security cameras, drones, media on campus, cell phones
- General Filming Restrictions
 - Live streaming
- General Audio Recording Restrictions
- Email & Social Media Monitoring



CAMERAS



- Cameras may not be used in locations where there is a “reasonable expectation of privacy”
 - DOJ guide on security technologies in colleges and universities (1999)
- Security camera footage is not covered under FERPA
 - Not an “education record”
- Ubiquity of cell phones



GENERAL FILMING RESTRICTIONS

- No filming permitted:
 - Restrooms
 - Individual offices
 - Other people’s homes
 - Dressing / locker rooms



- Exceptions:

- Entrances / exits (e.g., to create a timeline)
- Asset areas / cash handling
- Increased control sources (e.g., radiological)
- Certain research (e.g., animal)



GENERAL AUDIO RECORDING RESTRICTIONS

- No gathering audio from:
 - Eavesdropping
 - Remote recording (surreptitious)



- Exception:
 - Make the parties aware that they are being recorded
 - "This call may be monitored"

"lions and tigers and bears ...!"

- Social Media
 - BYOD
- Location Tracking
 - GPS / Geolocation (apps)
- Minors on Campus / Sport Camps
 - COPPA (web sites directed at kids)
 - Privacy management protocols
- FERPA Restrictions
 - "Nuclear Option"



COMPLEX WEB OF STATE BREACH LAWS



- All 50 states now have security breach notification laws
 - AL and SD became the last to do so as of March 2018
- At least 30 states, Puerto Rico and D.C. are currently considering measures that would amend these laws
 - Biometrics
- Some states' laws are limited to electronic information
 - Some also include paper
- Harm standards, safe harbors, AG/other notification(s), notification timeframes & other details vary



OPEN RECORDS

- DTH Media Corp. v. Folt (N.C. App., 2018)
 - Request for disclosure of records of persons having been found responsible for rape, sexual assault or any related or lesser included sexual misconduct (FERPA)
- Doe v. Univ. of Wash. (W.D. Wash., 2017)
 - Fetal tissue donation and research (injunction)
- Animal Legal Def. Fund v. Bd. of Regents Univ. of Wis. (Wis. App., 2017)
 - IACUC “notes for personal use” exemption



University of Colorado
Boulder | Colorado Springs | Fort Collins | Anschutz Medical Campus

Duke | OFFICE of
AUDIT, RISK & COMPLIANCE

Discussion?

Questions?



Contact:

- Kathleen Sutherland, Department of Internal Audit, University of Colorado
kathleen.sutherland@cu.edu
- Debi O'Connor, Compliance/Privacy Officer, University of CO Colorado Springs
doconnor@uccs.edu
- Holly Benton, Duke Privacy, Office of Audit, Risk & Compliance
holly.benton@duke.edu



University of Colorado
Boulder | Colorado Springs | Fort Collins | Anschutz Medical Campus

Duke | OFFICE of
AUDIT, RISK & COMPLIANCE
