Courtney Ingraffia Barton

Courtney is responsible for the development, implementation, and oversight of Hilton Worldwide’s Global Privacy Program. In this role she provides counseling and training on all aspects of consumer and employee privacy, partnering with Customer Marketing, Online Services, Human Resources, Information Technology and other members of the legal department to guide Hilton Worldwide’s global privacy practices and initiatives. Courtney is the Founder and Co-Chair of the Association of Corporate Counsel National Capital Region Data Privacy and Security Forum and serves on the Advisory Boards for the Georgetown Law School Cybersecurity Law Institute and the Information Governance Initiative. She is a graduate of Colby College, Tulane Law School and received an MPH from Harvard University. She is co-editor of the book, Managing ESI and E-Discovery (ABA, 2011).
Alan Raul is the founder and leader of Sidley’s highly ranked Privacy, Data Security and Information Law practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programs, data breaches, cybersecurity, consumer protection issues and Internet law. Alan’s practice involves litigation and counseling regarding consumer class actions, FTC, State Attorney General, Department of Justice and other government investigations, enforcement actions and regulation. Alan provides clients with perspective gained from extensive government service, as well. He previously served as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, and of the U.S. Department of Agriculture, and Associate Counsel to the President.

Alan serves as a member of the Privacy, Intellectual Property, Technology, and Antitrust Litigation Advisory Committee of the National Chamber Litigation Center (affiliated with the U.S. Chamber of Commerce). Alan also serves on the American Bar Association’s Cybersecurity Legal Task Force by appointment of the ABA President.
Agenda

• U.S. Legal Requirements
• International Requirements
• Data Security and Breaches
• Privacy and Cybersecurity Governance and Best Practices
• Additional Issues
• Issue Spotting
• Questions/Answers
Sources of U.S. Privacy Law and Regulation

- Federal statutes & implementing regulations, such as:
  - Privacy Act (applicable to US Government databases)
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Federal Trade Commission (FTC) Act (Section 5)
  - Electronic Communications Privacy Act (ECPA)
  - Computer Fraud and Abuse Act (CFAA)
  - Telephone Consumer Protection Act (TCPA)
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
  - Fair Credit Reporting Act (FCRA)
  - Communications Act
Sources of U.S. Privacy Law and Regulation

• State law
  – States Attorneys General / “Mini FTC Acts”
  – Tort law
  – State data breach notifications laws (including some specific to medical data)
  – State general data security/secure disposal laws
  – State specific data security laws (e.g., 201 MA 17.00 regulations from Massachusetts Office of Consumer Affairs and Business Regulations [MA 201])
  – State biometrics laws (Texas, Illinois)
  – State laws relating to social media privacy (employees)
  – State medical privacy laws
  – State genetic information privacy laws

• Private Litigants / Plaintiffs’ Bar
  – Hot trend: Class actions in the wake of a data breach
  – Hot trend: Marketing privacy class actions (use of fax, text, calls, online behavioral targeting/cookies)

• Industry self-regulation
  – E.g., online marketing opt-out choices (such as Network Advertising Initiative)
Federal Trade Commission

- Section 5 of FTC Act (15 USC §45(a)) prohibits “unfair or deceptive acts or practices in or affecting commerce”
- The FTC remains the leading data security regulator, and is the central regulator for general privacy issues
- The FTC has been particularly active recently on privacy issues domestically, and internationally
- Biggest recent themes out of the FTC include:
  - The FTC’s own enforcement/rulemaking authority
  - International data protection
  - Big Data
  - Children’s Privacy
  - New Technologies: Internet of Things, Facial Recognition
  - Data Security/Cybersecurity
**FTC Act (Section 5)**

• In April 2014, *Wyndham* decision (on MTD) upheld FTC authority to bring an unfairness or deception suit based on allegations of lax data security practices
  – Court acknowledged that FTC’s Section 5 was general, not specific, grant of authority, but this flexibility was particularly well suited to monitor fast moving technology and data practices
  – “the Court is unpersuaded that regulations are the *only* means of providing sufficient fair notice. … analogy to tort liability - where liability is routinely found for unreasonable conduct … especially since Hotels and Resorts itself recognizes how "quickly" the digital age and data-security world is moving”

• Appellate review pending
FTC Act (Section 5)

- FTC Settlements
  - American Apparel, Atlanta Falcons, Denver Broncos, Tennessee Titans, Level 3, BitTorrent, Charles River Labs, DataMotion, DDC Labs, Reynolds Consumer Products, Apperian, Baker Tilly, Receivable Management Services
    - Deceptive claims of Safe Harbor certification
  - Snapchat
    - Deceptive claims about “ephemeral” photos and videos
  - Fandango and Credit Karma
    - Deceptive claims about security of apps; inadequate security measures
  - TRENDNet
    - Deceptive claims re data security; inadequate security practices for Internet-enabled video equipment; “internet of things”
  - GMR Transcription Services
    - Deceptive claims re data security; inadequate security practices for personal information
Health and Human Services Office for Civil Rights (OCR)

- Enforces:
  - HIPAA Privacy Rule
  - HIPAA Security Rule
  - HIPAA Breach Notification Rule
  - Confidentiality provisions of the Patient Safety Act and Rule

- HIPAA Covered Entities and their Business Associates
  - The covered entity must have a written business associate contract or other arrangement with the business associate that establishes the permitted uses and disclosures of Protected Health Information and requires them to comply with the requirements to protect the privacy and security of PHI
  - Business associates are directly liable for compliance with certain provisions of the HIPAA Rules

- PHI/Protected Health Information
  - Individually Identifiable Health Information transmitted or maintained in any form by a Covered Entity or its Business Associate
HIPAA: Implications of Business Associate Relationships

• Uses/disclosures to Business Associates are permissible so long as:
  – The Business Associates are contractually bound to appropriately safeguard the information (through the use of a “Business Associate Agreement”);
    AND
  – The Covered Entity takes steps to remediate situations where its Business Associate fails to comply with privacy obligations.
The Children’s Online Privacy Protection Act (COPPA)

• Enforced by the FTC

• Regulates the collection, use and disclosure of personal information of children under 13 by operators of commercial websites or online services that
  
  (i) are directed to children under 13, or
  
  (ii) have actual knowledge that data is being collected from a child

• Operators must:
  
  – Describe data collection practices in privacy policy
  
  – Obtain prior parental consent for certain data collection
  
  – Maintain confidentiality, security, and integrity of data

• In addition to New Rules, FTC has been reviewing and approving/denying Safe Harbor methods
Fair Credit Reporting Act (FCRA)

- Promotes accuracy, fairness, and privacy of information in the files of consumer reporting agencies
- Any entity that uses a credit report or other FCRA covered consumer report to deny application for credit, insurance or employment, or take any other adverse action against you, must disclose:
  - The adverse action based on the credit report information and the name, address and phone number of the agency that provided the information
- Consumer Reporting Agencies may not give out information to an employer or potential employer without written consent
- The FCRA does provide for suits even against users of consumer reports
- Some states have further consumer reporting laws that may provide for more rights
- May apply to certain applications of Big Data analytics, and may serve as guide for prospective approaches to Big Data
  - Notice of adverse decisions based on consumer reports
  - Some limitations of what and when data can be used, and who can access
Electronic Communications Privacy Act (ECPA)

- Wiretap Act and Stored Communications Act, along with State wiretap laws, prohibit interceptions of certain communications

- Consent to intercept?
  - Remember all-party states, such as California

- These laws have broad implications
  - Customer service/call centers
    - Recording for quality assurance? Beep tones?
  - Employee monitoring
    - What employee notices are in place?
    - Expectations of privacy given permitted personal use?
  - Marketing initiatives
    - Targeted Advertising using content inspection (e.g., gmail/yahoo suits)
Telephone Consumer Protection Act (TCPA)

• Restricts telemarketing and the use of automated telephone equipment
  – Autodialers/robocalls, Automated messages, faxes, texts
  – Some restrictions for transactional messages as well
  – Established the Do Not Call Registry (honor requests for 5 years)
• The FCC requires prior written consent for all autodialed or prerecorded telemarketing calls to wireless numbers and for prerecorded calls to residential lines
• Requires all prerecorded telemarketing calls to allow customers to opt out of future calls of that nature through an “interactive, automated opt-out mechanism”
• Faxes must have specific cover page information – popular suits in the medical arena given health care sector’s continued use of fax machines
• TCPA litigation is a current favorite of the class action bar
  – Includes a private right of action for claims with statutory damages of up to $500 per call or actual damages for any violation
• New “clarifications” issued by FCC on July 10, 2015
CAN-SPAM Act

- Requirements for the use of commercial messages
  - Each violating email is subject to penalties of up to $16,000

- Commercial vs. Transactional messages & the “Predominant Purpose”

- Don’t use false or misleading header information

- Don’t use deceptive subject lines

- Identify the message as an ad

- Include your valid physical postal address

- Include a clear and conspicuous opt-out and honor opt-out requests
  - Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message and you must honor a recipient’s opt-out request within 10 business days for free

- Monitor what others are doing on your behalf
  - You can’t contract away your legal responsibility to comply with the law
  - Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible
Managing a Global Program

- Risk Profile
- New Law, Change to Existing Law, General Privacy Review
- Number and Type of Properties
- Number of Employees
- Data Protection Law
- DPA Registration (Yes/No)
  - If Yes, Registration Status
- Whistleblower Registration (Yes/No)
  - If Yes, Registration Status
- Data Transfer Issues (Yes/No)
  - If Yes, Mechanism and Status
- DPO Requirement (Yes/No)

- Breach Notification Law
- Works Councils? (Yes/No)
  - If Yes, Status of Negotiations for Policies Training and Hotline
  - Contact Information
- Policy Roll Out Status?
- List of On-Boarding Documents
- Anti-Spam Legislation
  - B to C Marketing/Consent Language
  - B to B Marketing/Consent Language
- Cookie Regulations
- Hotline Clearance (Yes/No)
  - Reporting Restrictions
Scope of the Proposed New EU Regulation

• Regulation will apply to a data controller in the EU or outside the EU where activities aimed at offering goods or services to individuals in the EU or that monitor individuals

• To determine whether a controller is offering goods or services in the EU, it should be ascertained if it is “apparent” that controller is envisaging offering services to individuals in the EU

• Regulation now envisages three types of data: personal data, anonymous data and pseudonymous data

• Processing of sensitive data such as health data is prohibited unless an exemption applies such as consent

• Personal data and pseudonymous data are subject to the Regulation – incentives included for using pseudonymous data
International Transfers: Safe Harbor, BCRs and Model Contracts

• The Fall of the U.S.- EU Safe Harbor?
  – Previous adequacy decisions (including the Safe Harbor) and decisions relating to the EU’s standard contractual clauses for transfer of data in force for only five years after the new regulation
  – Recent report from European Commission on the functioning of Safe Harbor with 13 recommendations to revise Safe Harbor
  – German and some other DPAs have been overtly critical of Safe Harbor

• The Rise of Binding Corporate Rules
  – Binding Corporate Rules appear heavily favored, although standard contractual clauses seem stable
  – Possibility of sector-wide adequacy determinations, such as for regulated sectors of the U.S. economy, such as healthcare, reinstated

• Model Contracts
  – Controllers and Processors
The “cyber threat is one of the most serious economic and national security challenges we face as a nation … America's economic prosperity in the 21st century will depend on cybersecurity . . . .”
Privacy and Data Security Risks

• **Information Assets**, including personal information, proprietary information and other trade secrets are a critical business resource
  – Foster operational efficiencies, research, product innovation, customer outreach, and a competitive edge
  – Accompanied by the potential for operational, legal and reputational risk

• **Whenever Data is Involved**, there may be legal implications
  – Hard external legal obligations from privacy/data protection laws around the world
  – Soft external legal obligations from industry standards
  – Soft external legal obligations from evolving case law
  – Internally imposed legal obligations that may be externally enforced (e.g., privacy policies)
  – Legal obligations laterally imposed (e.g., from contract)
The Cost of Getting It Wrong

• Compromise of Personal Information may lead to identity theft for affected data subjects
• Loss of Information Assets/Trade Secrets
• Litigation Exposure
• Regulatory Risk for data protection requirements as well as other general requirements (e.g., Securities and Exchange Commission [SEC])
• Time and Money
• Brand and Reputation
• Trust with Sensitive Information
• Loss of Competitive Standing
The Cost of Getting It Wrong

- **Target**
  - Target’s March 2015 10-k disclosed that “Since the Data Breach, we have incurred $252 million of cumulative expenses . . . .”

- **Anthem**
  - Several news outlets speculated that Anthem would deplete its $100 million cyber insurance coverage in notifying victims of the breach and providing credit monitoring.

- **Health Care Breaches generally**
  - A May 2015 global study of data breach costs sponsored by IBM and conducted by the Ponemon Institute found that “The average global cost of data breach per lost or stolen record is $154. However, if a healthcare organization has a breach the average cost could be as high as $363.”
  - A separate study by the Ponemon Institute in March 2015 found that the average cost of a data breach for the healthcare organizations sampled was estimated to be greater than $2.1 million.
  - The same study also found that criminal attacks on health care organizations have increased 125% compared to 2010, and “[f]or the first time, criminal attacks are the number one cause of data breaches in healthcare.”
Sources of Cybersecurity Guidance

• NIST Cybersecurity Framework
  – Identify, Protect, Detect, Respond, Recover
• Agency-specific guidance (e.g.):
  – Banking agencies
  – HHS/HIPAA security rule
  – Critical Infrastructure agencies (e.g., Dep’t of Energy)
  – SEC “Corp. Fin.” Disclosure Guidance; SEC Investment Management Division guidance; FINRA report
  – DOJ guidance
• State laws (e.g., Massachusetts)
• EU (e.g., ENISA guidance; UK guidance)
• Certifications/standard-setting Bodies (e.g., ISO, COBIT, SANS, etc.)
Department of Justice (DOJ) Cybersecurity Guidance


• Critical first step: implement cybersecurity plans/procedures
  – Identify valuable information assets
  – Detail key personnel for public communications, IT access, and legal questions
  – Determine critical IT components and information that must be preserved in responding to an incident
  – Assess how to forensically preserve data
  – Ensure appropriate training, data loss prevention measures, data backup measures, and intrusion detection
  – Develop procedures to notify data owners, customers, partners and law enforcement
DOJ Cybersecurity Guidance cont’d

• Do not use your communications systems to communicate about an incident
• Do not engage in active defense/ Hack Back
• Obtain legal counsel conversant in technology and laws governing electronic surveillance, privacy, and computer fraud in advance
• Engage in network monitoring, with appropriate mechanisms for pervasive consent from network users
• Develop points of contact with law enforcement in advance, contact them “immediately” after a criminal breach
• Provide notice to other victims
• Establish relationships with cyber information sharing organizations (Information Sharing and Analysis Centers [ISACs]
Information Sharing and Analysis Organizations [ISAOs])

• To respond to the cybersecurity threat, companies must:
  – understand their risks
  – identify applicable legal obligations (positive law, agency and public expectations, litigation exposure)
  – assign and allocate internal responsibility, accountability and resources
  – establish an effective system of internal cyber controls and information governance

• A comprehensive written information security plan is essential, and required (Massachusetts, etc.)

• Audit logging
  – HIPAA does not specify what activities should be logged
  – A proposed rule for access reports (accountings of disclosures) suggests that OCR expects date and time of access, identity of person accessing the information and what actions were taken (e.g., create, modify, view, print)
  – Retention of audit reports (as opposed to logs) for 6 years from the date of creation?
Legal Considerations

- Identify legal obligations; preserve privilege
- Keep up with fast-moving policy, public and litigation developments
- Data security laws in US and EU for personal information (MA, other states, etc.)
- Data breach notification requirements
- SEC disclosures and public filings
- Sector-specific regulatory requirements
- Industry/NIST cybersecurity standards
- Contractual obligations
- Do not “find and forget”
Board, CEO and GC Leadership on Cybersecurity

- Fiduciary Duties
- Regular reporting on threats, planning and execution
- Insist on testing the system (internal and penetration)
- Ask: How do we stack up against NIST Framework? Against peer companies? Against (relevant) government expectations?
- Assign clear responsibility for cybersecurity function, including senior internal staff and outside consultants
- Demand accountability
- Provide sufficient resources
Key Cybersecurity Questions to Ask

- Are we “critical infrastructure” operators?
- Do we have IP assets, trade secrets, account records, consumer data that could be subject to cyber-attack? Could our facilities be misused as part of an attack?
- What past incidents have we experienced? Are our incident response procedures effective and well understood throughout the organization?
- Do we have an up-to-date cybersecurity risk assessment in hand?
- Who is responsible for cybersecurity, and does he/she have sufficient resources?
- Is the Board of Directors adequately focused on cybersecurity? Has it established satisfactory internal controls and governance structures?
- What do we need to include in our SEC filings on cybersecurity?
- Do we know what existing and prospective laws apply to cybersecurity?
- Do we know what our contracts say about cybersecurity; do our existing customer / vendor contracts protect us on cybersecurity? What contractual obligations do we have?
- Do we have relevant government contracts? Do we have cleared persons?
- Are we participating in appropriate information sharing?
- Who is monitoring NIST developments and best industry practices?
Paper Trails and Planning

- Document organizational response to NIST
- Comprehensive internal cybersecurity program
- Written information security plan
- Incident response under direction of counsel
- Notification planning
- Business continuity planning
- Board briefing
- Secure relationships with vendors and third parties
- Engage forensic experts, PR consultants, lawyers – in advance – and ensure secure communications
Outside Resources

• Identify outside resources, including:
  – Forensic analysts to identify and remediate cyber-attacks
  – Cyber consultants to enhance cyber-control systems
  – Public Relations and communications specialists
  – Legal specialists
  – ISACs or ISAOs (Information Sharing and Analysis Centers/Organizations); industry associations
  – Government agencies for coordination and advisory purposes (“Here to help you”?)
    • Note DOJ recommendation of pre-existing FBI or Secret Service point of contact
    • Preserve Privilege!
Best Practices, Technology and Education

- Be aware of what practices are standard and which are state of the art
- Monitor Relevant Information Sharing and Analysis Center (e.g., FS-ISAC), Department of Homeland Security (DHS), NAIC, etc. alerts
- Keep up with fast-moving changes technology
- Assure up-to-date “patching”
- Consider cyber-insurance
- Internal education, training and raising individual awareness and responsibility
- Communicate periodic alerts on new and existing threats throughout organization
- Every employee and vendor is potential weak link
- Plan, deliberate, document and train
- Do not “find and forget”
Other Issues of Note

• Big Data
  – Ethical data practices

• Privacy by Design; Security By Design

• Privacy and Cybersecurity Due Diligence
  – Vendor management
  – Deals
  – Contracting for privacy and security

• Cloud Computing

• Internet of Things
  – Connected devices
  – Industrial Internet

• Workplace Privacy; Social Media; BYOD, etc.

• Drones
Getting Your Privacy House in Order

• Identify an owner

• Inventory your personal information

• Determine what laws apply

• Understand your process

• Define your policies and procedures

• Train, monitor, audit, repeat
Issue Spotting: Data Collection and Processing

- Limitations on the collection, use and disclosure of data may be present whether data is collected directly from a customer, from a third party business partner or vendor, or even from another department within your company.

- As a general rule, in addition to legal restrictions that may exist (e.g., disclosures of protected health data), data should be processed in accordance with privacy commitments.
  - Some privacy policies, for example, may have disclosed that the company would like to use the data collected for a variety of purposes.

- **Ask Yourself:**
  - Where is this data coming from?
  - Does this data trigger any special legal requirements or special precautions?
  - Is it being used as was expected when collected from the data subject?
  - Do any other third parties have rights in this data that limit what I want to do?
Issue Spotting for Privacy and Data Security Risks

- **Understand Your Privacy and Data Security Commitments**
  - E.g., What are our information security and privacy policies?
  - E.g., Are there any contractual limitations on data I want to use?

- **Spot the Issues**
  - E.g., What are the cybersecurity risks of working with this vendor?
  - E.g., What are data subjects privacy rights for this initiative?

- **Know Who to Ask**
  - E.g., Who knows how the data was collected and whether there are limitations on use?
  - E.g., Who do I call if I suspect a data breach?

- **Follow Up and Mitigate Risk**
  - E.g., Are we still holding on to data we don’t need?
  - E.g., Has an proposal evolved so I should reevaluate the privacy concerns?

- **Stay Informed**
  - E.g., What cybersecurity threats are in the news? Industry alerts?
  - E.g., Have relevant laws changed?
Questions?

Alan Charles Raul
Partner
Sidley Austin LLP
1501 K Street NW
Washington, D.C. 20005
202-736-8477
araul@sidley.com

Courtney Ingraffia Barton
Senior Counsel, Global Privacy
Hilton Worldwide
7930 Jones Branch Drive
McLean, VA 22102
703-883-5961
courtney.barton@hilton.com