WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WEBINAR

QuickLaunch University: Privacy and Data Security Considerations for Startups

APRIL 14, 2020

Speakers: Kirk J. Nahra and Rosemary G. Reilly

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1 CLE credit in California and New York*

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire live program. CLE credit is not available for those who watch on-demand webinar recordings.

WEBINAR

Speakers

Kirk J. Nahra
Co-Chair, Cybersecurity and Privacy Practice
WilmerHale

Rosemary G. Reilly
Partner, Corporate Practice
WilmerHale

Our Session Today

- Why you need to be considering privacy and security issues for your business
- A basic understanding of key privacy and data security principles
- An identification of key areas where these issues will matter to your company
- Big picture privacy and security issues for your consideration
- Where the law is going – and why this matters to you
- Your questions

Your Thinking Today

- Increasingly important issue in a broad range of industries and sectors, and for a growing range of kinds of information
- Front page news almost daily in our current crisis situation
- Your companies can be part of the solutions in this area – but more frequently these solutions must integrate privacy and security lessons and obligations
- And a failure to incorporate these considerations also is causing problems for creative and interesting and innovative companies

A Little History

- Privacy used to be only a constitutional law issue in law schools
- Dealt with abortion, birth control, Communist party membership, search and seizure
- Not really an issue for corporate America
- Started to become an issue involving personal data and consumers/individuals and their relationship to companies in mid-1990s
- Now an enormous compliance and regulatory issue across the country and the world, for companies in virtually all industries

Privacy Law Today

- Relevant if you have data about employees, customers, consumers or anyone else
- Personal data is being gathered in more and more places by more and more companies
- Concept of personal data also is growing, in the business world and in legislation/regulations
- Internet of Things generally, biometrics, facial recognition, location data, all kinds of advertising links

What Are We Talking About?

- Privacy – Laws, regulations and practices surrounding how personal data is used, gathered, maintained and disclosed
- Privacy is the area where there has been the most activity over the past decade, and where there are the most sensitivities and most tensions around the world

What Are We Talking About?

- Security – Laws, regulations and practices surrounding how personal information is protected from unintended and unpermitted activity – the practices that protect decisions made on privacy
- Security is moving from a best practice to a mainstream legal requirement, and there have been far more breaches, litigation and enforcement surrounding security than privacy

Cybersecurity

- Cybersecurity – protection of overall technological infrastructure
- Focused on national security and internet interconnections – which may or may not involve personal data
- Cybersecurity is broader than data security and narrower in some ways as well
- System operations/Interconnections
- Proprietary and commercial data as well

Basic Privacy Framework: US

- Large (and growing) number of laws and regulations, at state, federal and international levels
- Laws have (to date) been specific by industry segment (e.g., health care, banking) or by practice (e.g., telemarketing)
- Today, there is no generally applicable US privacy law covering all industries and all data
- Increasing complexity of regulatory environment

Basic Privacy Framework: US

- Detailed obligations for contracts with vendors
- Limited enforcement, although there are many agencies with enforcement authority
- Limited but growing range of litigation concerning privacy and security practices
- Increasing concern about “big data” and otherwise unregulated personal data
- Growing concerns about artificial intelligence and algorithms

Basic Privacy Framework: International

- Separate privacy and security rules related to data in and coming from foreign countries
- The rules usually are tougher in other countries than in US – more protective of individual privacy (where there are rules)
- An increasing number of countries do have privacy rules – and the rules are changing dramatically
- Significant disarray currently with changes in real time

Information Security Framework

- Security is now a separate legal requirement in the US – connected to privacy but with different rules and issues
- Security is a top issue today, with almost daily news stories and a tie to identity theft
- Security has moved from a business-driven “best practice” to a legal requirement in all industries.
- Visible and public breaches on a relatively consistent basis

The Major Laws

- Key Laws for regulated sectors – HIPAA (health care), GLB (financial institutions), FERPA (education)
- Telemarketing, CAN-SPAM
- Now GDPR and CCPA (with more to come)
- Permitted uses and disclosures (obligations for notice and/or choice)
- Individual rights

The Major Laws

- Enforcement and private litigation
- Security standards and security breaches
- Substantial government investigations and now litigation (particularly over breaches and specific laws with statutory damages)
- Enormous attention from legislatures and regulators across the country

Structural Reminder

- Why does this matter?
- Not all health information – only health information that has a defined connection to a “covered entity” (typically a health care provider or health insurer/health plan)
- Think wearables/Apple Watch/Fitbit/mobile apps
- No covered entity involved
- Lots of individual health information
- No HIPAA coverage

Structural Reminder

- Now think Apple/Aetna
- Apple and insurance giant Aetna have teamed up on an iPhone and Apple Watch app that provides rewards, including an option to earn a free Apple Watch, to members who engage in healthy behaviors like getting regular exercise and more hours of sleep. The new app, dubbed Attain, also provides Aetna members who sign up with nudges, such as to get an annual flu shot or take their medication on time

Why Does This Matter?

These issues are impacting a broad variety of areas for any company including:

- Overall compliance
- Litigation
- Mergers and acquisitions
- Product design
- Corporate strategy
- Business relationships
- Marketing

Some Questions For Your Consideration

Key issues to be thinking about

- Product design (e.g., collection, integration, security)
- What data are you collecting? Is it linkable to a person or device (or in some other way)?
- Data flows – what data are you generating?
- Where are you getting other data from? Did you (or your source) have the right permissions and rights?
- Sensitive data categories – health, financial, genetic, biometrics, facial recognition, location

Some Questions For Your Consideration

- Can you "aggregate" the data for analytics or product improvement?
- Can you legally or practically de-identify the data?
- What is being done with your data?
- What rights do you have in data?
- Are you interested in selling data?
- Where are you operating?

Some Questions For Your Consideration

- What happens at the end of a client relationship?
- Who are your customers and partners?
- Does your business model impact where you are regulated?
- Transactions (vendors and corporate activity)

The Future of Privacy Law

- Lots of states looking at a state law
- Unclear how many of these will happen and whether they will be similar to CCPA or not
- Watch other state laws on narrower categories – biometrics, facial recognition, location data
- Federal government also looking at a national law
- Has been almost zero likelihood this year, now certainly no chance

Future of Privacy Law

- Much higher likelihood in next administration – whoever it is
- Wildcard – 3-5 major states pass their own laws
- We can expect a significant debate once the current crisis ends
- Some current issues are adding to this debate (research, data analytics, location tracing)

Issues For The Current Debate

- Pre-emption
- Private right of action
- Individual rights
- Use and disclosures – opt-in/opt-out
- Simplicity – overlaps with other federal law as well
- Consistency with international approach

Some Things To Think About – An Example For Today

California Consumer Privacy Act – how is your health information protected/regulated?

1. HIPAA protected information (generally exempted from CCPA)
2. CMIA covered companies/information (generally exempted from CCPA)
3. Common Rule/Clinical research (generally exempted from CCPA)
4. CCPA – probably covers your health information if it isn't exempted
5. BUT CCPA doesn't cover non-profits
6. And CCPA doesn't generally cover employers and employee information
7. How can consumers, businesses and others deal with this?

A Different Approach

- GDPR – Broad principles establishing data privacy and security law across the EU
- Protects all personal information in all settings
- Application to a wide range of US companies
- Health care industry simply part of the overall legislation
- Health care data considered sensitive information with certain special restrictions
- <u>Not a recommendation but an alternative model</u>

Some Crisis Issues To Be Thinking About

- Employee privacy issues have become very significant – what can you disclose and collect about employees (and think about whether other individuals are relevant)
- Tricky balancing between rights of “sick” employees and rights of others
- Significant security concerns as work moves remote – make sure your team is trained and educated and that you are paying close attention to your systems

Key Steps

Do you know what kind of information you have and what happens to it?

- Evaluate any place in your company that you collect, store and disclose sensitive data (especially SSN and credit card information)
- New kinds of “sensitive” data – biometrics, locations data, genetics (and think about what’s next)
- Pay attention to employee data as well as customer data
- Can you identify where this information is disclosed?

Key Steps

Are you paying attention to the right rules?

- What are the rules that are applicable to you (and your customers)?
- Are you following the various marketing rules?
- Do you collect information from children online?
- Have you thought about your health care benefits program?
- Are you disposing of sensitive information properly?
- Have you told your employees how you monitor them?

Key Steps

Do you have an appropriate information security program?

- Is someone assigned this responsibility?
- Do you have documentation for a regulator?
- Does your program encompass paper and electronic information?
- Have you trained your employees on basic information security?
- Do you have appropriate contracts and oversight of vendors?

Key Steps

Are you ready to act if there is a problem?

- Do you know who is in charge?
- Do your employees know where to go in the event of a problem?
- Do you have a good program to identity and fix problems?
- Have you evaluated the requirements for security breach mitigation and notification?

Other Key Questions

- Have you thought about your relationships/strategies with your business partners?
- Have you thought about your relationships/strategies with your customers?
- Are you fully aware of the data you are collecting – and what do you consumers know about that?
- Can you support/justify your use and collection of data to an acquisition partner?

Questions?

Kirk J. Nahra
Co-Chair, Cybersecurity and Privacy Practice
WilmerHale
Kirk.Nahra@wilmerhale.com
202.663-6128
@kirkjnahrawork

Rosemary G. Reilly
Partner, Corporate Practice
WilmerHale
Rosemary.Reilly@wilmerhale.com