We Are Not Immune: Why Every Legal Practice Must Get Smart About Information, Privacy and Security. NOW.

Scot Ganow, Esq., CIPP/US

June 9, 2017

FARUKI

Scot Ganow, Esq., CIPP/US

- Privacy and Security Law
  - Information privacy compliance
  - Data security and breach response management
  - Risk assessment, audits, policy development
  - HIPAA, GLBA, FCRA, PCI-DSS, COPPA, FERPA
- Business & Transactions
- Intellectual Property

- 13+ years data privacy & compliance experience
- Certified Information Privacy Professional (CIPP)
- Adjunct Professor of Law, Univ. of Dayton
- Former Corporate Privacy & Ethics Officer

FARUKI

On the menu…

1. Start with the basics: data at risk
2. 2016: “The Year of the Breach”
3. State of Data Breach Litigation
4. Ethical obligations under Ohio Rules
5. A cautionary tale: Shore v. Johnson & Bell

…and time permitting….

6. So What’s Your Story?

FARUKI

What's personally identifiable information ("PII")?

- "Personally identifiable information" = privacy
- You must consider:
  - Direct identifiers; AND
  - Indirect identifiers

FARUKI

HIPAA's PII: Protected Health Information ('03)

- Names
- All geographic subdivisions smaller than a state (except for the first 3 digits of the zip code in some cases)
- Names of relatives and employers
- All elements of dates (except year) for dates directly related to an individual (e.g., birth date, admission date, discharge date, date of death) and all ages over age 89 and dates indicative of that age
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers

HIPAA's PII: Protected Health Information ('03)

- Medical record numbers
- Health plan beneficiary numbers
- Account numbers (Member ID's)
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URL)
- Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photos and any comparable images
- Any other unique identifying number, characteristic or code

In 2017, a lot more can be identifiable

- Longitude and Latitude (cell phone)
- Biometrics (thumb prints, facial recognition, retinal scans)
- Fitness devices
- Key stroke pressure
- Gait (walk)
- Pills (embedded with transmitters)
- “Internet of Things”

FARUKI

Beyond Privacy: Trade Secrets

Trade Secret Information

- Trade secrets only retain legal safeguards so long as they remain secret.
- Highly vulnerable to disclosure through anonymous means
- Mitigation: Take Down Requests (limited impact)
- Remedies: Injunctive Relief under State/Fed Law
  - Who to Sue?
  - Timing is Everything

Beyond Privacy: Trade Secrets (cont.)

- U.S. International Trade Commission has the authority to bar importation of goods resulting from unfair trade practices

- Protection: Apply for patent protection?
  - Secure protection
  - Requires disclosure

- Practice Tip: Better safeguards up front to keep it "secret"

FARUKI

Beyond Privacy: Patents

- March 16, 2013, America Invents Act : a first-inventor-to-file patent system.

- Prior Art under AIA

"any public disclosure, something in public use, on sale, or *otherwise available to the public anywhere in the world* in any language prior to the effective filing date of the claimed invention." §102(a)(1)

- Breach = public disclosure??

FARUKI

Prior Art Exceptions and Grace Period §102(b)

(1) DISCLOSURES MADE 1 YEAR OR LESS BEFORE THE EFFECTIVE FILING DATE OF THE CLAIMED INVENTION.—A disclosure made 1 year or less before the effective filing date of a claimed invention shall not be prior art to the claimed invention under subsection (a)(1) if—

(A) the disclosure was made by the inventor or joint inventor or *by another who obtained the subject matter disclosed directly or indirectly from the inventor* or a joint inventor; or

FARUKI

Beyond Privacy: Trademark & Copyright

- Generally less risk associated with breach as both require disclosure and evidence of use/ownership

- But still a cost…
  - Premature disclosure of product or brand launches
  - Disclosure prior to protections asserted
  - PR responses in the wake of a data breach involving unreleased material

2. 2016: "Worst Year Ever for Data Breaches"

Some Common Themes

- **People, people, people.**
  - Social engineering (SnapChat and NSA)
  - #1 Attack vector: Malware launched by Phish
  - Law Firm: Proskauer & Rose (W-2 phishing attack)
- **Most often the hack is not something new**
  - Trump Organization and OPM (patching)
  - Law Firm: Mossack Fonseca ("Panama Papers" breach)

3. The Litigation Landscape: Where Things Stand

- Private litigation is virtually inevitable when a major consumer data security breach occurs
- Costs are substantial even when an early dismissal obtained
- Obtaining early dismissal is becoming increasingly difficult as the plaintiff's bar explores new theories of relief

FARUKI

3. The Litigation Landscape: Themes

Breached Entity

- Failed to have adequate safeguards
- Failed to give affected timely notice of the potential compromise of their information
- Deceived consumers regarding adequacy of security

Plaintiffs

- Customers (class actions)
- Shareholders (if public company)
- Card brands and card issuers (if payment card data involved)

3. The Litigation Landscape: Theories of Liability

- Contract-Based Theories
- Negligence-Based Theories
- Common Law: invasion of privacy, bailment, misrepresentation, unjust enrichment
- Consumer Protection Statutes

FARUKI

3. Breach Litigation Landscape: Major Cases

- Clapper v. Amnesty Int'l, 133 S.Ct. 1138 (2013): "allegations of future injury are not sufficient" to establish Article III standing.

  BUT…

- Remijas v. Neiman Marcus, LLC, No. 14-3122 (7th Cir. 2015): "…plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information?..."

- Spokeo v Robins (U.S., May 2016)
  - Plaintiff must show "injury in fact" from Defendant's actions/inaction
  - Moreover, the Court emphasized, the injury needed to be both "concrete and particularized."

So what does this all mean?

- Current Law: Plaintiffs must show real harm caused by data breach to have standing
- Regardless, litigation costs time, money reputation, even with dismissal
- Even without litigation-breach response still costs time, money, reputation
- Cracks are in the wall of a quick dismissal for lack of standing

And in the Legal World…..

- Courts, firms and practitioners are subject to the same threats
- “One Stop Shop”
- Not always the ultimate target
- Reminder: All types of data, not just PII
  - Confidential client information
  - Trade secrets
  - Intellectual property
- Of course, an additional set of rules apply…

Professional Rule 1.1: Competence

- Ohio Rule 1.1: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation **reasonably** necessary for the representation. (emphasis added)

- Comment 8 to Rule 1.1: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (emphasis added)

Professional Rule 1.1: Competence

- ABA Cybersecurity Handbook: "[i]f a lawyer is not competent to decide whether use of a particular technology (e.g., cloud storage, public Wi-Fi) **allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help."**

- You cannot delegate responsibility for the security function.

Professional Rule 1.4: Client Communications

- Requires attorney-client communications, specifically “about the means by which the client’s objectives are to be accomplished.” Ohio Rule 1.4.(a)(2)

Professional Rule 1.6: Confidentiality

- "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." (Rule 1.6, emphasis added)

- Comment 18: "[f]actors to be considered in determining the reasonableness of the lawyer's efforts" include:

  - "the sensitivity of the information
  - the likelihood of disclosure if additional safeguards are not employed
  - the cost of employing additional safeguards
  - the difficulty of implementing the safeguards
  - the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." (emphasis added)

Rules 5.1 & 5.3: Supervision

- Rule 5.1(c): Responsibility for others/compliance with the Rules
- Rule 5.3: Lawyers and firms "shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that," first, "all lawyers in the firm conform to the Rules of Professional Conduct"
- 2013 Ohio opinion: Lawyers may use cloud services as long as they competently select an appropriate vendor, preserve confidentiality and safeguard client property, provide reasonable supervision of cloud vendors, and communicate with the client as appropriate. (Adv. Op. 2013-03)

Rules 5.1 and 5.3: Supervision

- ABA Cybersecurity Handbook: “rapidly evolving technology means that these factors cannot provide a ‘safe harbor.' "Instead, “[l]awyers should monitor and reassess the protections of the cloud provider as the technology evolves.”

But hang on a minute…

“Welcome to Pre-Breach, Jon Anderton”

Shore v. Johnson & Bell

- **April 2016:** Class Action filed v. Johnson & Bell by former clients; *Jason Shore & Coinabul v. Johnson and Bell LTD, Case 1:16-cv-04363, N.D. Ill. (April 15, 2016)*
- **Claims**
  - Legal malpractice (breach of contract)
  - Legal malpractice (negligence)
  - Unjust enrichment
  - Breach of fiduciary duty
- **December 2016:** Shore withdraws complaint, but successfully requests unsealing
- **April 2017:** Johnson & Bell sues Plaintiff's Counsel
  - Defamation : False claims re: firm's information security
  - Violation of ethics rules

Allegations

- Complaint: No verifiable breach of client information alleged
- Firm's alleged security failures

1. Firm's time keeping system was:
   - Improperly configured
   - Running out-of-date software ("Decades old")
   - Introduced "JBOSS exploit", as a result
2. Firm's virtual private network (VPN) was improperly configured and exposed to potential "middle man" exploit
3. E-mail system insecure
   - Obsolete encryption
   - Vulnerable to specific, known attacks

FARUKI

A cautionary tale and what we can learn

Claim 1: Legal malpractice/breach of contract

- Firm held itself out as authority in security (published article)
- Engagement letter representation to client

> "*Document Retention. During the course of the representation, J&B shall maintain a file on your behalf. The file may include material such as pleadings, transcripts, exhibits, reports, contracts, certificates, and other documents as are determined to be reasonably necessary to the representation ("Your File"). Your File shall be and remain your property. J&B may also include in the file its attorney work product, mental impressions, and notes (collectively "Work Product"). The Work Product shall be and remain the property of J&B."*

- Plaintiff: Clause "implicitly" warrants confidentiality using "reasonable methods."
- Insufficient safeguards = breach of contract clause
- Rules implicated: Confidentiality 1.6, Competence 1.1, Client Communications 1.4

FARUKI

A cautionary tale and what we can learn

Claim 2: Legal malpractice/negligence (in the alternative)

- Failed to implement industry standard data security measures which gave rise to vulnerabilities
  - Did not use a reasonable degree of professional care
  - Did not have or use the requisite skills to represent clients
- Firm had awareness of risks and issues/did nothing
  - Its own published articles
  - Its agreements
  - Panama Papers “DROWN” vulnerability
  - Never followed or used ABA’s “Member Cyber Alerts” from FBI
- Rules implicated: Confidentiality 1.6, Competence 1.1, Client Communications 1.4, Supervision 5.1

FARUKI

A cautionary tale and what we can learn

Claim 3: Unjust enrichment (in the alternative)

- Failed to implement industry standard data security measures which gave rise to vulnerabilities
  - Did not use a reasonable degree of professional care
  - Did not have or use the requisite skills to represent clients
- Clients paid attorneys fees which should have included security expenses
- Firm should return such fees for unjust enrichment
- Rules implicated: Competence 1.1, Client Communications 1.4

A cautionary tale and what we can learn

Claim 4: Breach of fiduciary duty (in the alternative)

- Firm failed to maintain a duty of confidentiality
- Firm failed to implement the reasonable safeguards to keep data confidential
- Clients paid attorneys fees are damages, as a result
- Rules implicated: Confidentiality 1.6, Competence 1.1, Client Communications 1.4

FARUKI

Case Take Aways

- **Show me the harm: Still need a "breach" (for now).**
- **Communications.** Carefully consider your written commitments in contract and in policy (internal and external). Think about HOW you communicate with your clients and the safeguards you use.
- **Confidentiality.** Security is indeed implied. You cannot promise confidentiality without safeguards.
- **Competence** requires you keep apprised of the technology's capabilities and risks and implement timely solutions for both.
- **Supervision.** You can delegate authority (whether third party service provider or employee with technology) but not responsibility security. Use administrative and technical safeguards to do so.
- **"Reasonable."** No set standards, but consider data type, cost, complexity, risk and nature of the information in selecting safeguards. (1.6)

Other Trends Impacting Firms: Assessments

- Client surveys and risk assessments
  - New clients
  - RFP
  - Existing clients, as required by insurers

- Cyber insurance coverage for firms
  - Risk assessment required, or helps reduce premium costs
  - Provides additional services beyond liability management

B. Get Your Story Straight: Know the Rules

A. No brainer? Yes, but often overlooked until trouble hits.

B. Review obligations under the law AND in your own agreements and policies with clients.

C. Review ABA Cybersecurity Handbook and PR for guidance

D. Complete an audit of your company's compliance with the rules
- What data do you have?
- Why do you have it?
- Where do you keep it?

E. Consider best practices and standards: ISO 27000 series and NIST

C. Data Governance is your Story.

A. Information: What, Where, How and Who Uses It

B. Safeguards

1. Administrative
2. Technical
3. Physical

C. Accountability & Management (It never ends)

Data Governance

Finding reasonable a balance between:

- Technology
- Data Use and Needs
- Security
- Empowerment
- Accountability

Chapter 1: Data Classification

- You cannot govern what you do not understand
- Define the data in external terms
  - Personally Identifiable Information (“PII”)
  - Protected Health Information (“PHI”) (HIPAA)
  - Non Public Personal Information (“NPI”) (GLBA)
  - Trade Secret, Patentable
- Define the data according to internal standard
  - High Risk, Medium Risk, Low Risk
  - Level I, II, III
  - Confidential, Public, Proprietary

Chapter 2: Data Mapping

- You cannot safeguard what you cannot locate
- Map of existing locations where PII/PHI is stored
  - Technical locations: Databases, servers, systems, cloud service providers
  - Physical locations: Office, floor, office buildings
- Map of existing data flows
  - Internal: Between locations
  - External: From internal locations to external locations

Chapter 3: Administrative Safeguards

- Drafting policies (the “why”)
- Drafting procedures (the “how”)
- Educate on policies and procedures
  - Regularly scheduled training sessions
    - Assessments
    - Evaluation of competency
  - Awareness program (there is a difference)

Never underestimate the value of an awareness program

- Target: Unverified e-mail with link clicked by a HVAC service provider employee

- Proskauer Rose (April 2016: W-2 Phish)

Don’t let your employee be “that guy”……

Or worse…. Use your work email to sign up for stuff.

Administrative Safeguards: Policies

Once you know where you data lives, you can construct safeguards, starting with policies

- Security Management Process Risk Analysis & Risk Management
- User Authentication Policies(ID, password, 2 factor auth.)
- Technology life cycle management
- Data retention, destruction & business continuity
- Mobile device use-wireless communication policy
- 3rd party audit process
- Employee training
- Social media use

Administrative Safeguards: Plans and Agreements

Incident Response Planning

- Establish Incident Response Team
  - Senior leadership, legal, marketing, PR and IT
- Draft an Incident Response Plan
- Test the Incident Response Plan

Agreements

- Independent contractors, contractors, vendors, other third parties
- Mandatory security obligations, to include notice for data breach
- Insurance (cyber policies or data breach coverage)

Chapter 4: Technical Safeguard Basics

- Encryption (complete with updates and key management)
- Antivirus, malware, intrusion detection systems, firewalls and monitoring
- Implementing administrative role-based access through technical solutions
- Third party implementation (Cloud service providers)
- Audit Controls
- System testing, patching and improvement

Chapter 5: Technical Safeguards: Practice 'Security in Depth'

- Must emphasize both perimeter based security AND layered security
- Multiple systems providing differing fail safes when other systems fail
- Must consider multiple pathways by which people can access data and safeguard each pathway
- Each person, device and technology represents another pathway that must be managed

Chapter 6: Physical Safeguards

- So often overlooked but still a viable way to breach an organization (think social engineering)

- Facility security (HQ, satellite, 3rd party providers)
  - Locks and Access Controls with Identity Management (passkeys)
  - ID Badges
  - Surveillance
  - Security staff

Chapter 7: Got it? O.K., Do it again!

Evaluation, Remediation and Maintenance

- Audit compliance with policies and procedures
  - Internal audits
  - External audits
  - System “stress tests”
  - Table top exercises
- Document all findings, corrections, revisions to policy

Ch. 8: Get Covered: A Good Story Helps

A. Consider insurance to offset the impact of data breach.

i. Liabilities
ii. Litigation
iii. Regulator inquiries

B. Consider additional services provided in some policies

i. Breach response manager (counsel)
ii. Think of opportunity costs and time spent on breach and not your business
iii. Breach response can be a marathon, not a sprint.

Ch. 9 WHEN an incident happens…

A. Take a breath, slow down (but only for a moment) and…

B. Use your incident response plan (yes, you should have one)

C. Convene your incident response team

D. TELL YOUR STORY: Follow your plan-just like you practiced. (yes, you should practice)

FARUKI

FARUKI IRELAND COX RHINEHART & DUSING PLL

Scot Ganow, Esq., CIPP/US

(937) 227-3716

sganow@ficlaw.com

@FICPrivacy

www.ficlaw.com