Cybersecurity and Legal Ethics

Gregory Hoffman, Esq.

gregorychoffmanesq@gmail.com

(201) 822-1365

Reasonableness Standard

- A Lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.
  - ABA Model RPC 1.6(c)
  - NJRPC 1.6(f)

Comment to RPC 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…”
- If a lawyer is not competent to decide whether use of a particular technology allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer.

Lawyers' Legal Obligations to Provide Data Security

- Data Security = The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Process-Oriented Approach

- Identify Information Assets
- Conduct periodic risk assessments
- Develop and implement and appropriate security program
- Provide training and education
- Monitor and Test Security Controls
- Review and adjust the security Program
- Oversee 3rd party service provider agreements

Information Security Involves Protection of:

- Information Systems – computer systems, networks, and software.
- Electronic records, data, messages, and other information typically recorded on, processed by, communicated via, stored in, shared by, or received from such information systems.

Three Categories of Protection Measures

- Physical Security Controls
- Technical Security Controls
- Administrative Security Controls

Physical Security Controls

- Designed to protect the tangible items that comprise the physical computer systems, networks, and storage devices that process, communicate, and store the data, including servers, devices used to access the system, storage devices, and the like.

- Intended to prevent unauthorized persons from entering that environment and to help protect against natural disasters.

- E.g. Fences, walls, locks, safes, alarm sensors, security guards

Technical Security Controls

- Involve the use of software and data safeguards incorporated into computer hardware, software, and related devices.
- Ensure system availability, control access to systems and information, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate.
- E.g. firewalls, intrusion detection software, access control software, antivirus, passwords, PIN numbers, smart cards, biometric tokens, and encryption processes.

Administrative Security Controls

- Written policies, procedures, standards, guidelines, and supplemental administrative controls to guide conduct, prevent unauthorized access, and provide an acceptable level of protection for computing resources and data.

- E.g. Personnel management, employee use policies, training, discipline, and informing people how to conduct day-to-day operations.

Three Ways to Break Down Each Category

- Preventative Security Measures
- Detective Security Measures
- Reactive Security Measures

Preventative Security Measures

- Designed to prevent the occurrence of events that compromise security.
- E.g. Putting a lock on a door, installing a firewall.

Detective Security Measures

- Designed to identify security breaches after they have occurred.
- E.g. smoke alarm, intrusion detection software

Reactive Security Measures

- Designed to respond to a security breach and typically includes efforts to stop or contain the breach, identify the party/parties involved, and allow recovery of information that is lost or damaged.

- E.g. Calling the police, shutting down a computer system after detection of an unauthorized user.

Basic Security Obligations

- Provide security for your data and your clients' data.
- Inform appropriate parties of security breaches that occur.

Duty to Provide Data Security

- Typically no guidance on what specific measures are required to satisfy legal obligations because security is a relative concept.

- Reasonable standard from RPC 1.6

Bell v. Mich. Council, 205 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005)

- Defendant owed plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure that security of their most essential confidential identifying information.

In re TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83 (D. Mass. 2007)

- Court allowed plaintiffs to proceed on a “negligent representation” claim based on the theory that the defendants made implied representations that they had implemented the security measures required by industry practice to safeguard personal and financial information.

Other Obligations

- Contractual
- Self-Imposed Obligations
- Obligations Attached to Clients

Types of Data to Secure

- Attorney-client data
- Financial Data
- Transaction Records
- Tax Records
- Personal Data
- Email

Federal Statutes

- CFPA, Consumer Financial Protection Act of 2010
  - 12 U.S.C. §§ 5531(a), 5536(a)(1)

- FISMA, Federal Information Security Management Act of 2022
  - 44 U.S.C. §§ 3541-3549

- GLB Act, Gramm-Leach-Bliley Act
  - 15 U.S.C. §§ 6801, 6805

NJ Statutes

- N.J. Stat. § 56:8-162 – Data Disposal/Destruction
- N.J. Stat. Ann. § 56:8-163 – Security Breach Notification
- N.J. Stat. Ann. § 47:1-16; §56:8-164 – Social Security Numbers

N.J. Stat. § 56:8-162

- A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.

N.J. Stat. Ann. § 56:8-163

- Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

N.J. Stat. Ann. § 47:1-16

- No person, including any public or private entity, shall print or display in any manner an individual's Social Security number on any document intended for public recording with any county recording authority.

ABA Formal Opinion 477R (May 22, 2017)

- While unencrypted e-mail may well be appropriate for routine communications including information of “normal or low sensitivity”, transmitting “highly sensitive” information might require more secure communications technology or even avoiding the use of electronic communications altogether.

RPC 4.4(b) Respect for Rights of Third Persons

- A lawyer who receives a document or electronic information and has reasonable cause to believe that the document or information was inadvertently sent shall not read the document or information or, if he or she has begun to do so, shall stop reading it. The lawyer shall (1) promptly notify the sender (2) return the document to the sender and, if in electronic form, delete it and take reasonable measures to assure that the information is inaccessible

RPC 4.4(b) (cont.)

- A lawyer who receives a document or electronic information that contains privileged lawyer-client communications involving an adverse or third party and who has reasonable cause to believe that the document or information was wrongfully obtained shall not read the document or information or, if he or she has begun to do so, shall stop reading it. The lawyer shall (1) promptly notify the lawyer whose communications are contained in the document or information (2) return the document to the other lawyer and, if in electronic form, delete it and take reasonable measures to assure that the information is inaccessible. A lawyer who has been notified about a document containing lawyer-client communications has the obligation to preserve the document.

Official Comment to 4.4 - Metadata

- Lawyers should be aware of the presence of metadata in electronic documents.
- “Metadata” is embedded information in electronic documents that is generally hidden from view in a printed copy of a document. It is generated when documents are created or revised on a computer.
- E.g. Information on the author of a document, the date or dates on which the document was revised, tracking revisions to the document, and comments inserted in the margins

Should You Look at Metadata Received?

- A lawyer who receives an electronic document that contains unrequested metadata may, consistent with RPC 4.4(b), review the metadata provided the lawyer reasonably believes that the metadata was not inadvertently sent.
- When making a determination as to whether the metadata was inadvertently sent, the lawyer should consider the nature and purpose of the document.
- A document will not be considered “wrongfully obtained” if it was obtained for the purposes of encouraging, participating, in, cooperating with, or conducting an actual or potential law enforcement, regulatory, or other governmental investigation.

ABA Formal Opinion 06-42: Review and Use of Metadata

- Counsel sending or producing electronic documents may be able to limit the likelihood of transmitting metadata in electronic documents.
- A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata also may be able to send a different version of the document without the embedded information.
- E.g. send it in hard copy, create an image of the document and send only the image (this can be done by printing and scanning), or print it out and send it via facsimile.

Fed. R Civ. P. 26(b)(5)(B)

- *Information Produced*. If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

Amgen, Inc. V. Hoechst Marion Roussel, Inc. 190 F.R.D. 287 (D. Mass. 2000)

- "This approach empowers courts to consider a number of circumstances relating to the inadvertent production, including (1) the reasonableness of the precautions taken to prevent inadvertent disclosure, (2) the amount of time it took the producing party to recognize its error, (3) the scope of the production, (4) the extent of the inadvertent disclosure, and (5) the overriding interest of fairness and justice. Thus, depending on the totality of these factors, the court may rule either that the inadvertent disclosure has effected a waiver of the privilege or that the privilege remains intact."