



# Protecting Client Communications in a Digital World

*University of North Dakota School of Law*

*April 5, 2019*

Tracy Vigness Kolb

Meagher & Geer, Bismarck ND

# Perspective

Google





“By 2010, we as a species were creating more data per day than we did from the beginning of time until 2003. By 2015, 76 exabytes of data will travel across the Internet every year” – Bruce Schneier



- An exabyte is a billion billion bytes
- “To put it in human terms, an exabyte of data is 500 billion pages of text” – Bruce Schneier

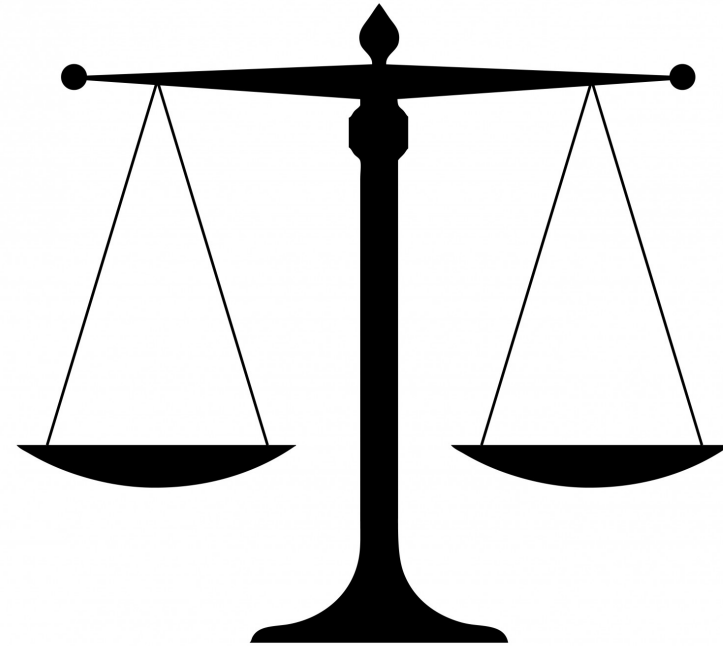


Lawyers are  
connected to the  
Internet



Risks and threats to  
information security

Lawyers are not  
immune from the risks  
and the threats





## Information Security Risks to Lawyers & Law Firms

- Law firms have large amounts of valuable information that includes confidential client data
- Law firms are perceived as easy targets

In 2011, FBI warned: Hackers see attorneys as a back door to the valuable data of their clients

Failed security

=

Data breaches

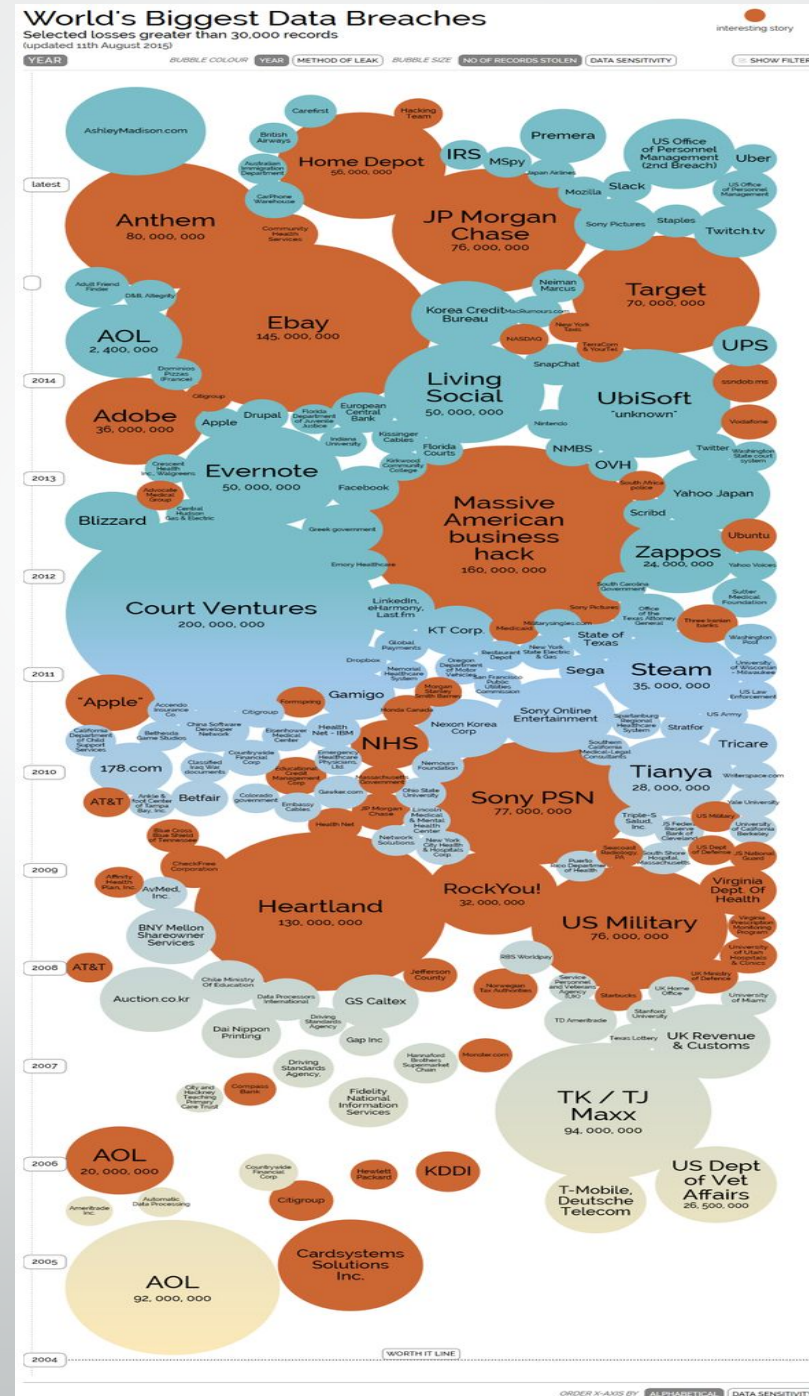




# Information is beautiful

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Average total cost of data breach in U.S. is \$6.7 million, or \$217 per lost or stolen record



# Law Firm Incidents

- Former law firm paralegal pled guilty to downloading firm's electronic trial plan for an asbestos case and offering to sell it to opposing counsel
- A college student temporary employee of a document management/production service provider of a law firm pled guilty to theft of trade secrets of law firm client
- Former law firm IT employee pled guilty to theft of computers from the law firm that he sold on eBay
- Former law firm partner sued by former law firm for allegedly installing software that allowed continued access to law firm files and then taking thousands of client files using Dropbox
- Hackers stealing closing funds in real estate transactions by intercepting lawyer-client emails through spearphishing scams
- Lawyer pays \$750 ransom for release of computer files
- Law firm pays \$2,500 ransom in bitcoin for release of computer files
- Securities broker pled guilty to insider trading with information stolen from law firm provided the broker by a lawyer friend within the firm
- Attempted scammer "spoofing" of clients with phone calls that trick caller ID into displaying their attorneys' phone numbers, followed by instructions to send money to the attorney
- Non-law firm: \$750,000 phishing email involving employee of a large health care entity who opened an email with an attachment that contained malicious malware, comprising the IT system and resulting in access to the records of 90,000 patients

# Information Security Threats to Lawyers and Law Firms

- Causes

- Malicious and criminal
  - Insider/outsider threats
- Human error
- System and IT glitches

- Types

- Lost and stolen devices
- Social engineering and phishing
- Improper disposal
- Impermissible access and disclosure
- Ransomware
- Vendor insecurity
- Hacking

# ABA Commission on Ethics 20/20

- Studied the impact of technology on the legal profession
- Determined the regulation of lawyers should be updated in light of how technology has transformed the practice of law



# The Technology Amendments to the North Dakota Rules of Professional Responsibility (Eff. 3/1/16)

ABA Technology Amendments Model Rules of Professional Conduct <sup>^</sup>		
Proposed by Ethics Commission (By Subject Matter)	Approved by ABA	Adopted by North Dakota Supreme Court
<b>Technology: Confidentiality</b>		
Rule 1.0 Terminology	✓	✓
Rule 1.1 Competence	✓	✓
Rule 1.4 Communication <sup>^^</sup>	✓	
Rule 1.6 Confidentiality	✓	✓ <sup>^^^</sup>
Rule 4.4 Respect for Rights of Others	✓	✓ <sup>^^^</sup>
<b>Technology: Client Development</b>		
Rule 1.17 Sale of Law Practice	✓	✓
Rule 1.18 Duties to Prospective Client	✓	✓
Rule 7.1 Communications Concerning a Lawyer's Services	✓	
Rule 7.2 Advertising	✓	✓
Rule 7.3 Direct Contact with Prospective Clients	✓	✓
<b>Lawyer Mobility</b>		
Rule 1.6 Confidentiality	✓	
Rule 5.5 Unauthorized Practice of Law	✓	✓ <sup>^^^^</sup>
New Model Rule-Practice Pending Admission	✓	
New Model Rule-Admission on Motion	✓	
<b>Outsourcing</b>		
Rule 1.1 Competence	✓	✓
Rule 5.3 Responsibilities Regarding Nonlawyer Assistants	✓	✓
Rule 5.5 Unauthorized Practice of Law	✓	✓ <sup>^^^^</sup>
<sup>^</sup> A second set of proposals was made by the Ethics Commission and approved by the ABA in February 2013 (Model Rule for Registration of In-House Counsel, Model Rule on Pro Hac Vice Admission, and an amendment to Model Rule 8.5 Disciplinary Authority). These were not adopted by the North Dakota Supreme Court.		
<sup>^^</sup> The last sentence of Comment [4] to Model Rule 1.4, which stated— “[c]lient telephone calls should be promptly returned or acknowledged”—was replaced with the following language: “Lawyers should promptly respond to or acknowledge client communications.” Its approval was not recommended by North Dakota’s Joint Committee on Attorney Standards because the comments to North Dakota’s Rule 1.4 adequately explain a lawyer’s responsibility to communicate with a client.		
<sup>^^^</sup> A new sentence was added at the end of Comment [17] of Model Rule 1.6: “Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.” Comment [17] pertains to transmission of confidential information whereas Comment [16] of Model Rule 1.6 pertains to storage of confidential information. The new sentence to Comment [17] was not included in the proposed amendments to North Dakota’s Rule 1.6 counterpart, Comment [19]. However, the other amendments to Rule 1.6 were adopted, including the addition of a nearly identical sentence to Comment [18] of North Dakota’s Rule 1.6.		
<sup>^^^^</sup> Rule 4.5(a) of N.D. R. Prof. Cond. is the counterpart to Model Rule 4.4(b).		
<sup>^^^^</sup> A limited clarifying amendment was adopted, but not Model Rule 5.5 amendments as approved by the ABA.		

# Technology Competence

- Protect and Maintain Client Confidences
  - Rule 1.1 Cmt. 5 (Competence)
  - Rule 1.6(d) (Confidentiality)
- Ensure Others Protect and Maintain Client Confidences
  - Rules 1.1 (Competence)
  - Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants)

# The Technology Amendments Takeaways

- Increase level of technology and security awareness
- Understand the new obligations as duties to secure client confidences
  - A duty to store, transmit, and outsource securely
  - Sources of the duty (ethical rules, federal and state laws and regulations, contracts, clients)
- Rules 1.1 and 1.6
  - Take competent and reasonable measures to safeguard client information
  - Applies to use of all technology (computers, mobile devices, network servers, cloud computing, and outsourcing)
- Rules 1.1 and 5.3
  - Before entrusting client confidences to others, make sure you know and understand the measures that will be used to protect and secure the confidences
  - Written confidentiality agreements





# Principles of an Information Security Program

- Comprehensive Security Must Address People, Policies, and Technology

- See the big picture
- Know the law and your regulator
- Designate someone with responsibility for information security
- Conduct a risk assessment
- Develop, implement, and maintain an information security program
- Manage your vendors
- Educate and train the entire workforce
- Consider cybersecurity insurance
- If you need help, get help

“The wealth of confidential data maintained in lawyers’ computers and information systems faces substantial and very real security risks. It is critical for all lawyers to understand and address these risks to ensure they comply with their legal, ethical, and regulatory obligations to safeguard client data.”

--ABA Cybersecurity Legal Task Force



“What we really need in IT is someone who has super powers.”

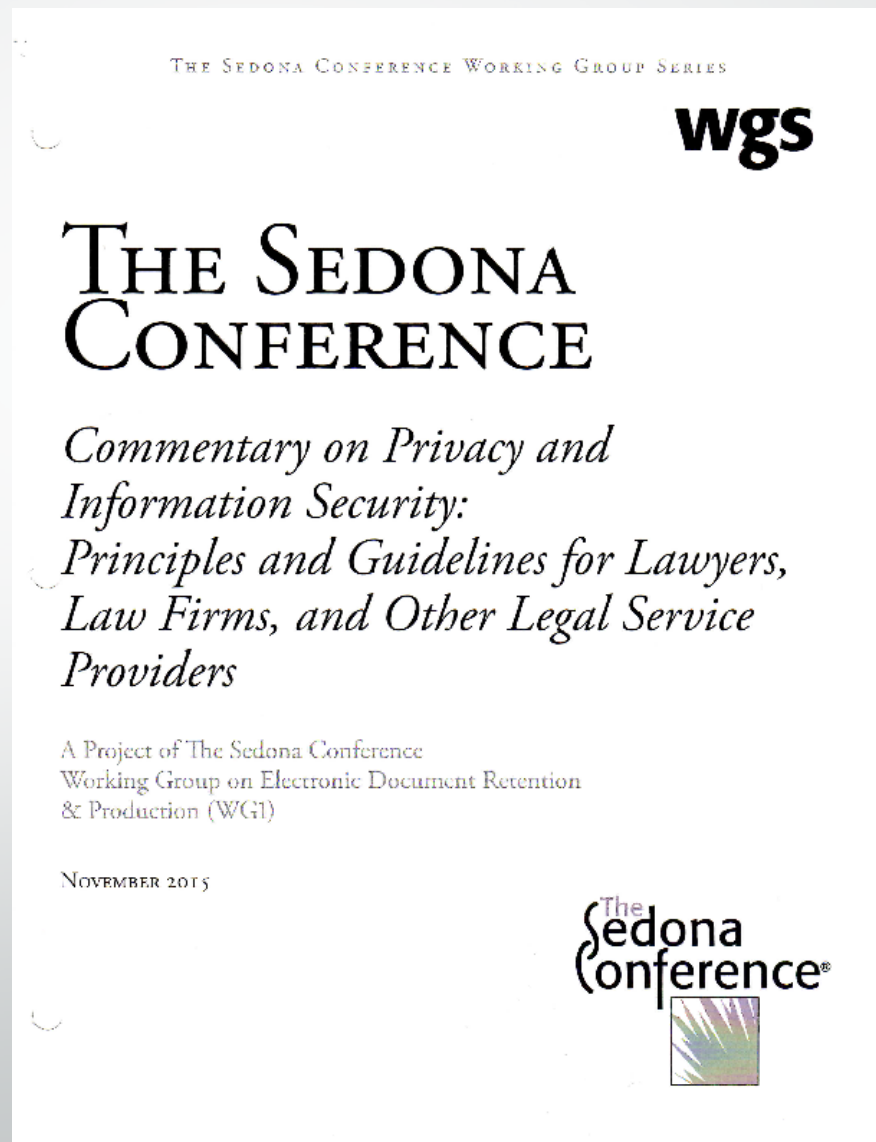
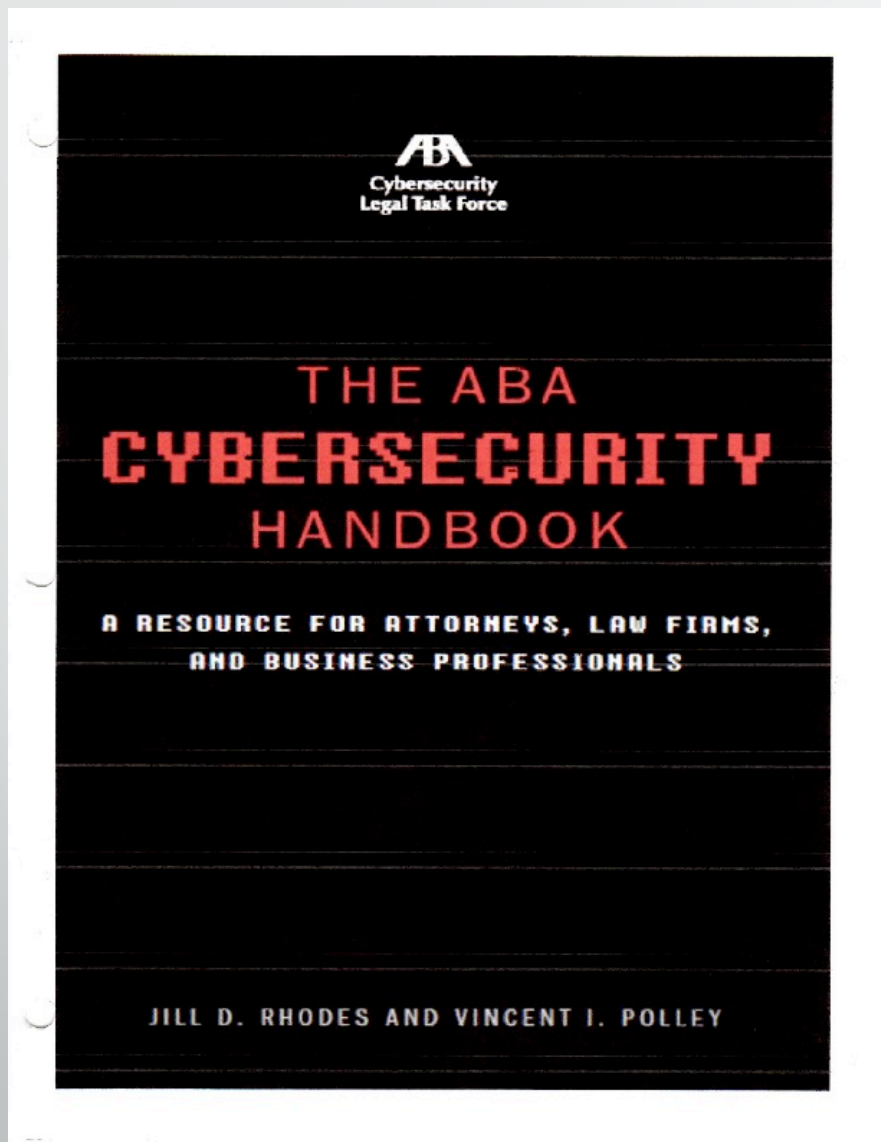
# Individual Lawyer Obligations

- Undertake education and training for basic technology competence
  - And stay updated and current
- Implement reasonable security measures to safeguard data on your devices
  - Mobile device tools
    - Laptop locks, remote wipe and encryption software
  - Password protection
    - Strong passwords (12 to 16 characters that include numbers, letters, and characters)
    - Multifactor authentication
  - No social media use/disclosure involving client data/communications
  - No public WiFi use
  - No unsanctioned/unsecured cloud storage involving client data/communications
  - Proper disposal practices

If you need help,  
get technology  
expertise




# Legal Resources



# Contact Information

Tracy Vigness Kolb  
701.333.0638  
tkolb@meagher.com





Any views or advice offered in this publication are those of its authors and should not be construed as the position of the University of North Dakota School of Law.

“This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought”—from a declaration of the American Bar Association.