Constitutional Communications Jonathan Stribling-Uss, Esq.
info@concomms.org

Legal Security Requirements for Attorneys Handling Client Data

Attorneys, and the private sector as a whole, are facing a crisis of data insecurity. The 2014 Ponemon Data Breach Study interviewed 1166 Information Technology (IT) professionals and 1110 end-user employees in a representative cross section of public and private entities in the US and Europe. They concluded that 67 percent of IT Professionals self-reported their organization experienced the loss or theft of company data over the past two years and only 22 percent of employees reported that their organization was able to tell them what happened to lost, data, files, or emails. There are a number of steps that attorneys must take to address concerns about data security of their organizations or clients. Unified security planning and encryption are the most important first steps. This article addresses the current legal and ethical requirements for Attorneys to engage with digital technology, with a focus on the default encryption of client data.

Both Nevada and Massachusetts have legally mandated encryption as part of their consumer protection regulations. The Massachusetts Attorney General has been very active in enforcing consumer data protection. In July 2014, the Attorney General, enforced a civil penalty of $150,000 against the Women & Infants Hospital of Rhode Island (“WIH”) to resolve allegations that it lost unencrypted data. This legal action demonstrates that the Massachusetts Attorney General is aggressively engaged in enforcing both Federal and Massachusetts information security law against out-of-state entities who insecurely store the personal data of Massachusetts residents.

Massachusetts information security law, M.G.L. c. 93H, applies to “persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts.” The law applies to all private businesses including lawyers and law firms and requires that an organization have a written security plan that includes "to the extent technically feasible, . . . encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly." The organizational program also must include "[e]ncryption of all personal information stored on laptops or other portable devices." Covered “personal information” includes Social Security numbers, driver’s license numbers, state- issued identification card numbers, financial account numbers and credit card numbers. This law has been enforced against out-of-state businesses having sufficient minimum contacts with the Commonwealth of Massachusetts.

Nevada also has a robust data protection law with two principal sets of provisions. First, Nevada gives the Payment Card Industry Data Security Standard ("PCIDSS"), an industry standard developed by a private rule-making body, the force of law in the state. The PCIDSS aspect of the law requires all data collectors who do business in the state of Nevada and that accept a payment card in connection with a sale of goods or services must maintain the ir personal data securely. The second set of provisions requires encryption of personal information during electronic transmission or while in storage on data storage devices. The transmission provisions of the law require that a "data collector doing business in this State to whom subsection 1 does not apply [i.e., that is not required to comply with the PCIDSS] shall not . . . [t]ransfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission."

In addition to state-mandated legal schema, attorneys have a clear ethical responsibility to protect client information. Rule 1.6 of the Model Rules of Professional Responsibility states that, “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.” As the comments to the section reads, the “fundamental principle in the client-lawyer relationship is that, in the absence of the client’s informed consent, the lawyer must not reveal information relating to the representation.”

In 2012 the ABA modified the language of the applicable rule to impose an explicit obligation on attorneys to take positive steps to protect the confidentiality of information concerning their clients and cases. Each state bar has its own interpretation of how to define “reasonable effort.” Pennsylvania’s state bar, for example, has defined reasonable effort in a way that specifically encourages attorneys to regularly use encryption to protect their clients.

Business people are already transitioning to encryption en masse. A global survey of nearly five thousand businesses found encryption use has increased six percent in the past year to the point where 35 percent of organizations now have an encryption strategy applied consistently across the entire enterprise.[1] In the United States, encrypted traffic has jumped from 2.29 percent of all peak hour traffic before 2013 to 3.8 percent in 2014, and in Latin America it has gone from 1.8 percent to 10.37 percent.[2] More than ten global publications have embraced encrypted “dropboxes” for first contact with new sources, including The New York Times, The New Yorker, The Washington Post, and The Guardian.[3]

Law firms and attorney associations have been slow to secure their systems and are leaving themselves open to adverse legal action and significant fees as a result. State laws mandating encryption and uniform organizational security planning for attorney-client information are an important first step to real security and ethical responsibility in the information age.

[1] “Encryption use continues to grow”, www.net-security.org/secworld.php?id=16340 see also http://www.reuters.com/article/2014/02/11/fl-thales-idUSnBw115819a+100+BSW20140211

[2] “Encrypted Web Traffic More Than Doubles After NSA Revelations” www.wired.com/2014/05/sandvine-report/

[3] SecureDrop, https://freedom.press/securedrop