Encryption is Now Cheap and Simple and May Be Ethically Required

May 6, 2016

District of Columbia Bar

Presenters: Sharon D. Nelson, Esq. and John W. Simek
President and Vice President, Sensei Enterprises, Inc.
703-359-0700 www.senseient.com
snelson@senseient.com; jsimek@senseient.com

David G. Ries
Clark Hill PLC
Pittsburgh, PA
dries@clarkhill.com
John W. Simek
Sensei Enterprises, Inc.
Fairfax, VA
jsimek@senseient.com

Contents

Encryption is Now Cheap and Simple and Ethically Required … ~~Maybe~~[1]

Encryption is a topic that most attorneys don't want to touch with a ten-foot pole, but it is becoming a more and more important part of security. Encryption is an electronic process to protect the security and confidentiality of data. While an increasing number of attorneys are using encryption, many attorneys use excuses like "I don't need encryption," "it's too difficult," and "it's too expensive." These excuses are misplaced: attorneys need encryption and easy to use (after setup) and inexpensive (sometimes free) encryption solutions are available today. While attorneys will sometimes need technical assistance to install and set up encryption, it's generally easy from there.

Some more recent ethics opinions are now concluding that encryption may be a necessary safeguard in appropriate circumstances. The ethics rules and opinions and legal requirements set minimum standards. Attorneys should provide stronger safeguards as a matter of sound professional practice and client service. It has now reached the point where all attorneys should generally understand encryption, have it available for use when appropriate, and make informed decisions about when encryption should be used and when it is acceptable to avoid it.

1. Why Attorneys Need Encryption

Encryption can provide strong protection for stored data (on servers, desktops, laptops, tablets, smartphones, portable devices, etc.) and transmitted data (over wired and wireless networks, including the Internet and e-mail).

For example, a joint U.S. / UK research team has written that full disk encryption is so effective that law enforcement and federal agencies are complaining that they are unable to retrieve encrypted data in criminal investigations. Federal courts are struggling with the issue of whether compelled disclosure of passwords and passphrases for decryption is prohibited by the Fifth Amendment. British Prime Minister David Cameron, FBI Director James Comey, an Assistant Attorney General in the U.S. Department of Justice, and a group of state attorneys general have called for legally required back doors to encryption that would be available to the U.S. government for national security and law enforcement. They have complained that Apple and Google cannot provide access to encrypted iPhones, iPads, and Android devices because they no longer store decryption keys, leaving them with users.

There has been enhanced attention to encryption since the disclosure of widespread surveillance by the NSA and advocacy by tech companies, privacy advocates, security professionals, and Edward Snowden that encryption should be used to protect against this surveillance (as well as other threats). In October of 2015, the Obama administration announced that it will no longer pursue a legally required back doors in the U.S. Following the attacks in Paris and San Bernardino, there have been renewed calls for legally mandated back doors, despite the fact that there is no evidence to date that encryption had any impact on the attacks. Security professionals and technology companies, including Apple CEO Tim Cook, have strongly opposed back doors because they could work for hackers, criminals and oppressive governments as well as for national security and law enforcement.

---

[1] For more detailed information, see Sharon D. Nelson, David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015).

Protection of stored data on portable devices is a good example of why attorneys need encryption. After the high-profile theft from an employee's home of a Department of Veterans Affairs laptop and external hard drive containing personal information on more than 28 million veterans in 2006, security guidelines for federal agencies added the requirement of encryption of all data on laptops and portable devices, unless it is classified as "non-sensitive." That was ten years ago.

In January 2007, 18 laptops were stolen from the offices of a law firm in Orlando, Florida. The laptops were reportedly protected by encryption, and the incident received very little publicity. In discussing this incident, the SANS Institute, a leading information security organization, noted, "[l]aptop thefts aren't going away, but by this time next year, this type of item (laptop stolen, but the data was protected) shouldn't be newsworthy." That was more than nine years ago.

In one data breach report in 2011, a Maryland law firm lost an unencrypted portable hard drive that contained medical records of patients in a lawsuit against its client hospital. One of the law firm's employees took the hard drive containing backup data home with her. This was the firm's method of ensuring that it had an off-site backup. She took the light rail system home and left the drive on the train. When she came back a few minutes later, it was gone. Backup is a good practice, but not if it's done in a way that exposes confidential data. If the drive had been encrypted, it would have had a strong level of protection. As it was, it had little or none. It is not uncommon for backup software to have the ability to encrypt the backed-up information. Generally, it is just a simple matter to check an option for the backup to be encrypted.

In another example in 2014, an external hard drive was stolen from the trunk of the car of an employee of a law firm with an operations base in Atlanta. It contained confidential information about clients. It was not encrypted. It happened again in April of 2015, when an attorney's laptop was stolen on a trolley in San Diego. These examples are almost certainly the tip of the iceberg. We have informally heard of numerous additional instances where law firm laptops, smartphones, tablets and portable devices have been lost or stolen and were not protected with technology such as encryption.

As these examples demonstrate, encryption is particularly important for laptops and portable media. A lost or stolen laptop or portable device that is encrypted is protected unless the decryption key has been compromised. As discussed below, Verizon has called encryption a security no-brainer.

Attorneys also need encryption because electronic communications can be intercepted (during transmission and storage) and wired and wireless network can be intercepted or accessed. Cyberspace is a dangerous place!

2. The Ethics of Encryption

Attorneys' use of technology presents special ethics challenges, particularly in the areas of competence and confidentiality. Attorneys also have common law duties to protect client information and may have contractual and regulatory duties. These duties to safeguard information relating to clients are minimum standards with which attorneys are required to comply. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service.

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.

Model Rules 1.1 and 1.6: Competent and Reasonable Safeguards

The duty of competence (ABA Model Rule 1.1) requires attorneys to know what technology is necessary and how to use it. The duty of confidentiality (ABA Model Rule 1.6) is one of an attorney's most fundamental ethical responsibilities. Together, these rules require attorneys using technology to take competent and reasonable measures to safeguard client data. This duty extends to all use of technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

The Ethics 20/20 amendments to the ABA Model Rules in 2012 include addition of the following language (underlined) to the Comment to Model Rule 1.1 Competence:

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>…

As of December 23, 2015, 20 states have adopted this new comment to Model Rule 1.1, some with variations from the ABA language.[2]

The amendments also added the following new subsection (underlined) to Model Rule 1.6 Confidentiality of Information:

> <u>(c) 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.</u>

This requirement covers two areas – inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop, or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, producing privileged documents or data in litigation, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

The amendments also include the following changes to Comment [18] to this rule (underlined):

> **Acting Competently to Preserve Confidentiality**
>
> [18] Paragraph (c) requires a <u>A</u> lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against <u>unauthorized access</u> <u>by third parties and against</u> inadvertent or unauthorized disclosure by the lawyer or other persons <u>or entities</u> who are participating in the representation of the client or who are subject to the lawyer's supervision <u>or monitoring</u>. See Rules 1.1, 5.1 and 5.3. <u>The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors 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, and 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the</u>

[2] www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html.

> loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

This Comment provides some high level guidance for determining competent and reasonable safeguards. As discussed above, the following factors should be applied:

> Factors 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, and 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).

This is a risk-based approach that is now standard in information security. The analysis of whether encryption is required for attorneys should be viewed under this requirement for competent and reasonable measures using this risk based approach.

Encryption for Electronic Communications: "Special Security Measures"

Discussion of whether attorneys are ethically required to use encryption have focused primarily on e-mail, starting in the 1990s. For example, an ABA ethics opinion in 1999 and several state ethics opinions concluded that "special security measures," like encryption, are not generally required for confidential attorney e-mail.[3] However, these opinions should be carefully reviewed because, like Comment 19, they contain qualifications that limit their general conclusions. In addition, more recent ethics opinions, discussed below, are increasingly recognizing that encryption may be a required safeguard in some circumstances.

The Ethics 2000 revisions to the Model Rules, over 10 years ago, added Comment 17 [now 19] to Rule 1.6. This comment requires reasonable precautions to safeguard and preserve confidential information during electronic transmission. This Comment, as amended in accordance with the Ethics 20/20 recommendations (underlined), provides:

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may

---

[3] E.g., ABA Formal Opinion No. 99-413, *Protecting the Confidentiality of Unencrypted E-Mail* (March 10, 1999) ("based upon current technology and law as we are informed of it …a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a)…" "…this opinion does not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.") and District of Columbia Bar Opinion 281, "Transmission of Confidential Information by Electronic Mail," (February, 1998), ("In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.")

require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. 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.

This Comment requires attorneys to take "reasonable precautions" to protect the confidentiality of electronic communications. Its language about "special security measures" has often been viewed by attorneys as providing that attorneys never need to use "special security measures" like encryption.[4] While it does state that "special security measures" are not generally required, it contains qualifications and notes that "special circumstances" may warrant "special precautions." It includes the important qualification - "if the method of communication affords a reasonable expectation of privacy." However, as discussed below, there are substantial questions about whether Internet e-mail "affords a reasonable expectation of privacy."

Respected security professionals for years have compared unencrypted e-mail to postcards or postcards written in pencil.[5] A June 2014 post by Google on the *Google Official Blog*[6] and a July 2014 *New York Times* article[7] use the same analogy – comparing unencrypted e-mails to postcards and encryption to envelopes.

Reasonable expectation of privacy?

[4] Encryption is a process that translates a message into a protected electronic code. The recipient (or anyone intercepting the message) must have a key to decrypt it and make it readable. E-mail encryption has become easier to use over time. Transport layer security (TLS) encryption is available to automatically encrypt e-mail between two e-mail gateways. If a law firm and client each have their own e-mail gateways, TLS can be used to automatically encrypt all e-mails between them. A virtual private network is an arrangement in which all communications between two networks or between a computer and a network are automatically protected with encryption.

[5] E.g., B. Schneier, *E-Mail Security - How to Keep Your Electronic Messages Private,* (John Wiley & Sons, Inc. 1995) p. 3; B. Schneier, *Secrets & Lies: Digital Security in a Networked Work*, (John Wiley & Sons, Inc. 2000) p. 200 ("The common metaphor for Internet e-mail is postcards: Anyone – letter carriers, mail sorters, nosy delivery truck drivers - who can touch the postcard can read what's on the back."); and Larry Rogers, *Email – A Postcard Written in Pencil*, Special Report, (Software Engineering Institute, Carnegie Mellon University 2001).

[6] "Transparency Report: Protecting Emails as They Travel Across the Web," *Google Official Blog* (June 3, 2014) ("…we send important messages in sealed envelopes, rather than on postcards. …Email works in a similar way. Emails that are encrypted as they're routed from sender to receiver are like sealed envelopes, and less vulnerable to snooping—whether by bad actors or through government surveillance—than postcards.")
http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html.

[7] Molly Wood, "Easier Ways to Protect Email From Unwanted Prying Eyes," *New York Times* (July 16, 2014) ("Security experts say email is a lot more like a postcard than a letter inside an envelope, and almost anyone can read it while the note is in transit. The government can probably read your email, as can hackers and your employer.")
www.nytimes.com/2014/07/17/technology/personaltech/ways-to-protect-your-email-after-you-send-it.html?_r=0.

"The common metaphor for Internet e-mail is postcards: Anyone – letter carriers, mail sorters, nosy delivery truck drivers - who can touch the postcard can read what's on the back."
Bruce Schneier 1995

Email – A Postcard Written in Pencil
Larry Rogers 2001
SEI - Carnegie Mellon University

"Emails that are encrypted as they're routed from sender to receiver are like sealed envelopes, and less vulnerable to snooping—whether by bad actors or through government surveillance—than postcards."
***Google Official Blog* June 2014**

"Security experts say email is a lot more like a postcard than a letter inside an envelope, and almost anyone can read it while the note is in transit."
***New York Times* July 2014**

Encryption is being increasingly required in areas like banking and health care. Newer laws in Nevada[8] and Massachusetts[9] (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. The 2009 Healthcare Information Technology and Clinical Health (HITECH) Act enhanced HIPAA security requirements, extended them directly to business associates, and added a new breach notification requirement. Encryption is included as an "addressable" requirement, which means that it or an alternative must be implemented or a written explanation provided to explain why it is not needed.[10] In addition, the Federal Trade Commission has brought a number of enforcement actions against businesses based on allegations that they failed to take reasonable measures to safeguard the privacy and security of personal information about consumers. In over half of them, settlements required the businesses to employ additional safeguards, including encryption of personal information in transmission and storage.[11]

As the use of encryption grows in areas like these, it will become more difficult for attorneys to demonstrate that confidential client data that they transmit needs lesser protection.

Comment 19 to Rule 1.6 also lists "the extent to which the privacy of the communication is protected by law" as a factor to be considered. The federal Electronic Communications Privacy Act[12] and similar state laws make unauthorized interception of electronic communications a crime. Some observers have expressed the view that this should be determinative and attorneys

---

[8] Nev. Rev. Stat. 603A.010, *et seq.*

[9] Mass. Gen. Laws Ch. 93H, regulations at 201 CMR 17.00.

[10] See, 45 CFR Parts 160 and 164.

[11] Patricia Bailin, "Study: What FTC Enforcement Actions Teach Us about Features of Reasonable Privacy and Data Security Practices," *The Privacy Advisor* (Sept. 19, 2014), https://privacyassociation.org.

[12] 18 U.S.C. §§ 2510 et seq.

are not required to use encryption. The better view is to treat legal protection as only one of the factors to be considered.

Consistent with the questions raised by security experts about the security of unencrypted e-mail, some ethics opinions express a stronger view that encryption may be required. For example, New Jersey Opinion 701 (April, 2006), discussed above, notes at the end: "where a document is transmitted to [the attorney]… by e-mail over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access."[13] This was over nine years ago.

California Formal Opinion No. 2010-179, also discussed above, notes that "encrypting email may be a reasonable step for an attorney in an effort to ensure the confidentiality of such communications remain so when circumstances call for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous."

An Iowa opinion on cloud computing suggests the following as one of a series of questions that attorneys should ask when determining appropriate protection: "Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?" Iowa Ethics Opinion 11-01.

A Pennsylvania ethics opinion on cloud computing concludes that "attorneys may use e-mail but must, under appropriate circumstances, take additional precautions to assure client confidentiality." It discusses encryption as an additional precaution that may be required when using services like web mail. Pennsylvania Formal Opinion 2011-200.

"The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue [ethics] opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required." ABA, *Eye on Ethics* (July 2015)

Texas Ethics Opinion 648 (2015) takes the same approach:

> In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication.

It includes examples of circumstances where encryption may be required.

Summarizing these more recent opinions, a July, 2015 ABA article notes:[14]

---

[13] File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip uses encryption to protect security. It is generally easier to use than encryption of e-mail and attachments. However, the protection can be limited by use of weak passwords that are easy to break or "crack."

[14] Peter Geraghty and Susan Michmerhuizen, "Encryption Conniption," *Eye on Ethics, Your ABA* (July 2015) www.americanbar.org/publications/youraba/2015/july-2015/encryption-conniption.html.

> The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue [ethics] opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required.

In addition to complying with any applicable ethics and legal requirements, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients (preferably in an engagement letter or other writing) about the nature of communications that will be (and will not be) sent electronically and whether or not encryption and other security measures will be utilized.

It has now reached the point (or at least is reaching it) where all attorneys should have encryption available for use in appropriate circumstances.

3. Encryption Overview

Encryption is the conversion of data from a readable form, called plaintext, into a form, called ciphertext that cannot be easily understood by unauthorized people.
Decryption is the process of converting encrypted data back into its original form (plaintext), so it can be understood.
Encryption uses a mathematical formula to convert the readable plaintext into unreadable ciphertext. The mathematical formula is an **algorithm** (called a cipher). Decryption is the reverse process that uses the same algorithm to transform the unreadable ciphertext back to readable plaintext. The algorithms are built into encryption programs – users don't have to deal with them when they are using encryption (except for sometimes having to choose an algorithm from a list when encryption is originally set up).
This graphic shows the basic steps:

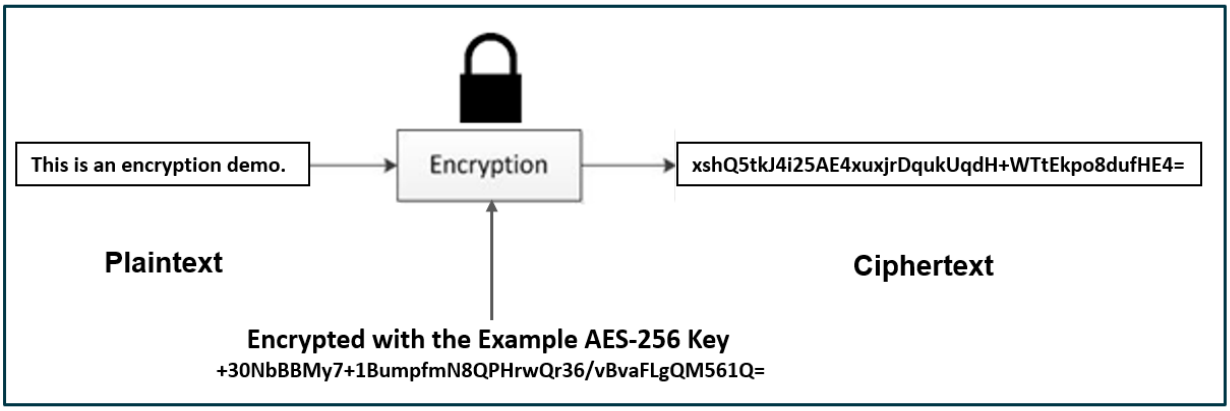
Encryption keys are used to implement encryption for a specific user or users. A key generator that works with the selected encryption algorithm is used to generate a unique key or keys for the user(s). A key is just a line or set of data that is used with the algorithm to encrypt and decrypt the data. Protection is provided by use of the algorithm with the unique key or keys.
The process is called **secret key** or **symmetric key encryption** where the same key is used with an algorithm to both encrypt and decrypt the data. With secret key encryption, it is critical to protect the security of the key because it can be used by anyone with access to it to decrypt the data. The public key can be distributed to anyone because it can be used only to encrypt.
Here is an example of a secret key for a commonly used algorithm called the Advanced Encryption Standard-256 (AES-256) algorithm. The same key is used to both encrypt and decrypt the data.

+30NbBBMy7+1BumpfmN8QPHrwQr36/vBvaFLgQM561Q=

Example AES-256 Key

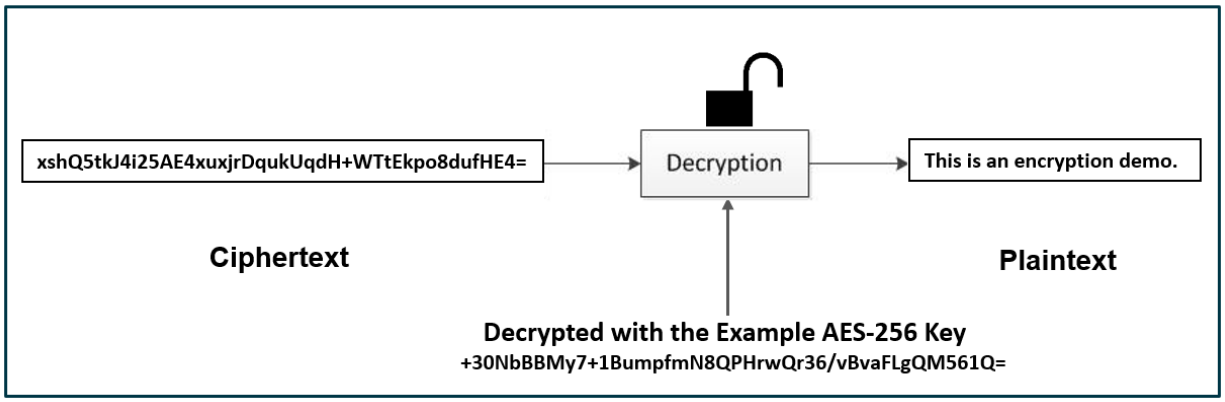
Where a **key pair** is used, one to encrypt the data and a second one to decrypt the data, the process is called **asymmetric encryption**. For this kind of encryption, a key generator is used to generate a unique key pair, one for encryption (a public key) and the other for decryption (a private key). With key pairs, it is critical to protect the private decryption key since anyone with access to it can decrypt the data.

Let's look at a simple example of its application. A short line of readable plaintext, "This is an encryption demo," becomes unreadable ciphertext when this key is used with the algorithm in an encryption program.



Simple Example of Encryption

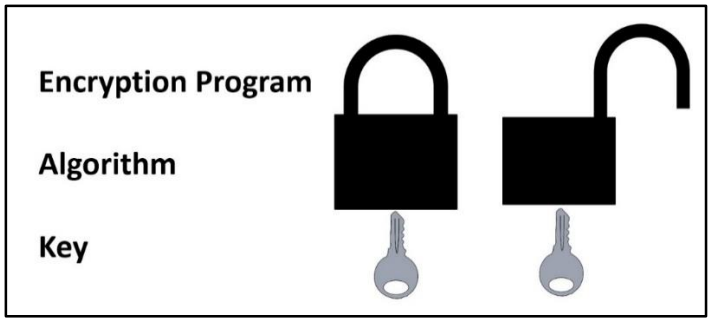
The same key must be used with the algorithm in an encryption program to convert the ciphertext back to readable plaintext.



Simple Example of Decryption

Symmetric key encryption is frequently used to protect data stored on servers, laptops, portable media, etc. The key is frequently used and stored on a single computer or mobile device where providing the key to someone at a remote location is not necessary. It is difficult to use symmetric key encryption for communications because it is a challenge to securely share the key with the recipient.

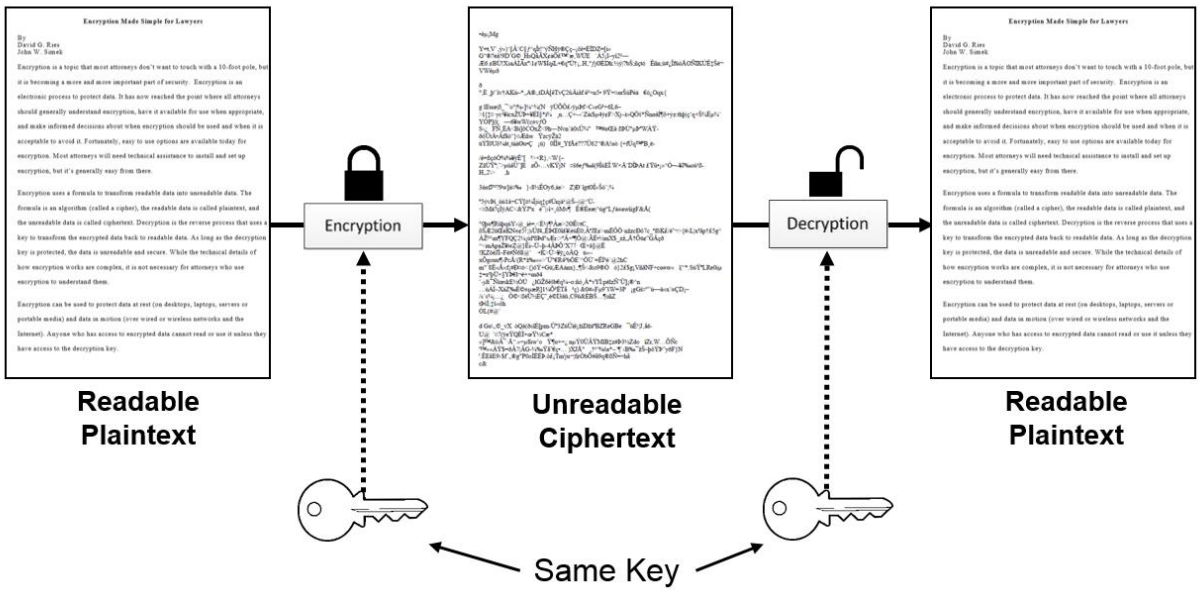
The following illustration provides a simplified analogy to show how the encryption process works. The lock is like an encryption program, the internal mechanism is like the encryption algorithm, and the encryption key or keys are like a physical key or keys.



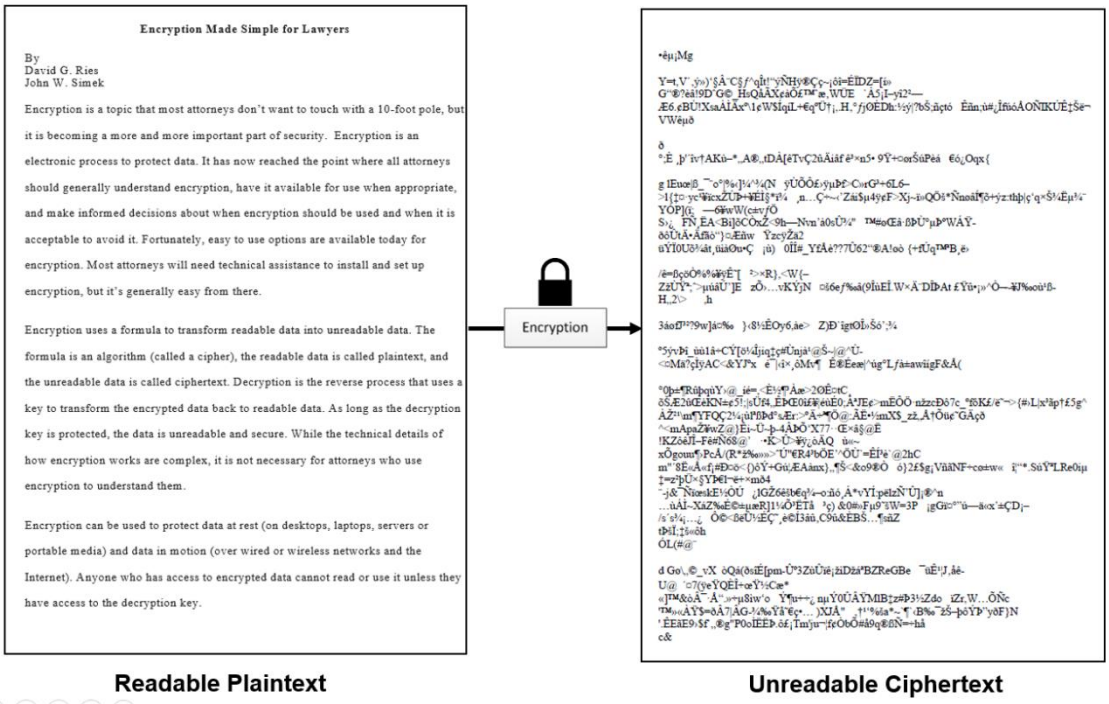
A Simplified Overview

Fortunately, users don't have to deal with keys during everyday use of encryption. When they log on with the correct password or passphrase, the program automatically accesses the key to decrypt the data. When they log off or shut down, the data is automatically encrypted.

The following is a longer example - a draft of an article written by the authors. A single key is used to encrypt the article. The same key is necessary to convert it back to plaintext.

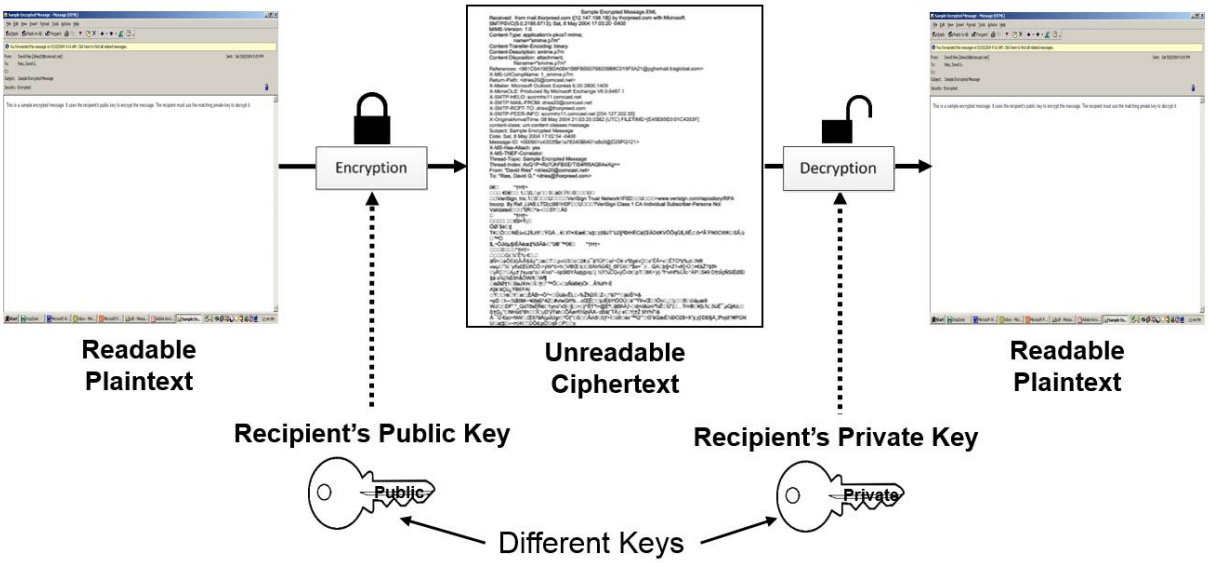


Here's an enlarged view of the plaintext and ciphertext:



Enlarged Example: Symmetric Key Encryption

Asymmetric encryption uses a key pair instead of a single key - one key (a public key) is used to encrypt the data and a second one (a private key) is used to decrypt the data. Key pairs are frequently used for encrypted communications. The sender uses the recipient's public encryption key to encrypt the communication. The public key cannot decrypt it; only the decryption key can do that. The recipient uses the decryption (private key) to decrypt the data.
Graphically, the process works this way:



Example of Public Key Encryption

This is a brief overview of symmetric and asymmetric encryption and how it works. Attorneys do not have to understand the details or the involved mathematics. As noted above, encryption can protect both data at rest and data in motion. After encryption has been set up, it's generally automatic or point and click.

Encryption can be inexpensive – even free. Apple's iPhones and iPads and Google's Android smartphones and tablets include encryption capability. Windows (business versions) and Apple's OS X now have built-in encryption. All of them are free with the respective operating systems. Many portable drives and USB thumb drives also include built-in encryption.

4. Laptops and Portable Media

The attributes that make laptops and portable devices useful also make them very dangerous from a security perspective: They're compact and portable. Add to that the fact that their costs have been decreasing over the years, their capacities have been dramatically increasing, and they have become more and more compact. Laptops are available with 2 TB (terabyte) and larger hard drives. USB thumb drives with capacities of 1 TB or more are now available. Portable hard drives of 1 TB or more are now available. A massive amount of data, in compact media, can be easily lost or stolen. With these devices, attorneys and employees can lose or steal the equivalent of a truckload of paper pages or more.

Not properly protected, laptops and portable media can be recipes for a security disaster. One survey reported that 70 percent of data breaches resulted from the loss or theft of off-network equipment (laptops, portable drives, PDAs, and USB drives). Strong security is a must. Encryption is now a standard security measure for protecting laptops and portable devices—and attorneys should be using it.

Encryption Basics

There are two basic approaches to encrypting data on hard drives: full disk encryption and limited encryption. As its name suggests, full disk encryption protects the entire hard drive. It automatically encrypts everything and provides decrypted access when an authorized user properly logs in. Limited encryption protects only specified files or folders or a part of the drive. With limited encryption, the user has to elect to encrypt the specific data.

There are also three kinds of encryption for protecting laptops and portable devices: hardware encryption, encryption in operating systems (such as Windows and Apple OS X), and encryption software.

Hardware Full Disk Encryption

All hard drive manufacturers now offer drives with hardware full disk encryption built in. The major laptop manufacturers all offer models with these drives. Hardware encryption is generally easier to use and administer than encryption software. Some examples are Seagate Secure (www.seagate.com) and Hitachi Self-Encrypting Drives (www.hgst.com). Secure use simply requires enabling encryption and setting a strong password or pass phrase. The contents of the drive are automatically decrypted when an authorized user logs in. It is automatically encrypted when the user logs off or the laptop is turned off.

Because most encryption programs are tied to a user's password, secure passwords or pass phrases are essential, and a forgotten password can lead to lost data. Automatic logoff, after a specified time, is critical so that unencrypted data will not be exposed if a user goes away from a computer or forgets to

turn it off. In an enterprise environment, like a law firm, access by an administrator, ability to reset passwords, backup, and key recovery are essential. Installing encryption and administering it, particularly in a large enterprise, can be a challenge.

Encryption in Operating Systems

Current business versions of Windows and current versions of Apple OS X have built-in encryption capability.

Windows Vista Enterprise and Ultimate and Windows 7 Enterprise and Ultimate, and Windows 8, 8.1 and 10 Professional and Enterprise include an encryption feature called BitLocker. BitLocker works below the Windows operating system and encrypts an entire volume on the hard drive. This means that when the drive is encrypted, the encryption protects the operating system, as well as all software and data on the drive. For versions of Windows that do not support BitLocker, software encryption, discussed below, can be used.

On versions before Windows 8.1, BitLocker required either a computer that is equipped with a Trusted Platform Module (TPM) chip or use of an external USB drive to hold the decryption key. A TPM module is a security chip on the computer's motherboard that supports encryption. If a user plans to use BitLocker on a computer, it is important to select one that has a TPM chip the meets the current specification. Check the hardware requirements for the version of Windows that you are using and compare it with the specifications for the desktop or laptop. Or ask someone for advice – the major PC manufacturers have chat features on their websites to answer questions about their products. Use of a key on a USB drive is less secure because encryption can be defeated if an intruder gains access to the USB key.

With Windows 8.1 and 10, there's another alternative for BitLocker with computers that don't have a TPM chip. It can be set up directly on the computer, but it requires a pre-boot passphrase that accesses the decryption key. This means that a user has to enter a pre-boot passphrase, then log into Windows. A user can set up the same passphrase for both, but it has to be entered twice, once for pre-boot and once for logging in.

A recent article[15] in *The Intercept* noted that if you login to a Windows 10 computer using your Microsoft account, it is likely that your computer automatically uploaded a copy of your recovery key to Microsoft. You can login to your OneDrive using your Microsoft account and see a list of recovery keys backed up to your account. As previously mentioned, securing access to your encryption keys is a very important part of protecting confidential information. You should probably delete any keys backed up to OneDrive and maintain control of your own backup recovery keys.

The business versions of Windows also include an encryption function called Encrypting File System (EFS). It allows encryption of files and folders. An authorized user who is logged in has access to decrypted data. It is encrypted and unreadable to anyone else (unless they can defeat the login process). EFS is considered a fairly weak encryption method that is easily cracked using forensic tools. You are better off using BitLocker or one of the third-party encryption products discussed below.

---

[15] Micah Lee, "RECENTLY BOUGHT A WINDOWS COMPUTER? MICROSOFT PROBABLY HAS YOUR ENCRYPTION KEY," https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key (December 28, 2015).

Setup of both EFS and BitLocker is fairly technical. For most attorneys, it will be necessary to obtain technical assistance to implement them.

OS X has built-in file encryption in FileVault. Newer versions have full disk encryption available in FileVault 2. Follow Apple's instructions for turning it on. After a password is set, it just requires turning on the FileVault button in System Preferences. Recent advances have attacked Apple's encryption scheme, and the Passware software suite claims to be able to defeat FileVault 2 in less than an hour.

Third-party Encryption Software

Some commonly used third-party encryption software products for hard drives include those offered by Symantec (PGP and Endpoint; www.symantec.com), McAfee (Endpoint Encryption; www.mcafee.com), Check Point (ZoneAlarm DataLock; (www.zonealarm.com), Dell Data Protection (www.dell.com), WinMagic (SecureDoc; www.winmagic.com), and Sophos (SafeGuard; www.sophos.com). Most of these vendors have options available for Macs.

Portable Drives

Hardware-encrypted drives and encryption software are available for USB drives and portable hard drives. Microsoft's BitLocker to Go can be used to encrypt portable devices. Individual USB drives with built-in encryption capability are also available, such as the IronKey (www.imation.com), Kanguru Micro (www.kanguru.com), Kingston (www.kingston.com), and SanDisk Cruzer Professional and Cruzer Enterprise (www.sandisk.com). The IronKey is a favorite of the authors. It includes strong encryption, wiping if the wrong credentials are entered too many times, and has strong physical construction. As an added bonus, several of the models contain a password management application called Identity Manager, which stores all your 14+ character passwords in a secured, encrypted "vault." Of course you can store any length password, but the current recommendation is 14 or more characters.

To avoid the loss of data, it is important to understand how the encryption works, to back up data that is encrypted, and to keep a copy of the recovery key in a secure place. Enterprise controls are available to centrally manage encryption in law firms and other enterprises.

5. Smartphones and Tablets

Smartphones and tablets are basically small computers, with substantial computing power and high storage capacity. Like laptops and other mobile devices, they can be easily lost or stolen and should be protected with encryption.

BlackBerry devices (www.blackberry.com) have long been the "gold standard" for security, although its market share has substantially declined. If you use the BlackBerry Enterprise Server (BES), the communications are automatically encrypted. Encrypting the device itself is accomplished by enabling Content Protection. You can find that choice by navigating to Options > Security Options > Encryption. This is where you will set encryption for the device memory, encryption strength, contacts, media files, and expansion memory card. In addition, you will need to set a password for the phone as well as the inactivity timer to lock the phone. The password and time-outs are set by going to Options > Password. A lot of law firms use BES to manage their BlackBerry devices. This centralized management will push the desired security settings to the phones with no user interaction.

For iPhones and iPads (www.apple.com), hardware encryption was implemented in iOS 4. All files are automatically encrypted when the iPhone or iPad is lock coded and decrypted when the device is unlocked. It provides limited protection unless Simple Passcode is turned off, Require Passcode is turned on, and a strong pass code is selected. Require Passcode should be set for a short time and Erase Data should be turned on. iOS also includes a feature called Data Protection. It secures e-mails and attachments stored on the device and data in other apps that are designed to work with it.

Android OS (www.android.com) has included encryption for tablets (starting with Honeycomb) and for phones (starting with Ice Cream Sandwich). Earlier versions require third-party apps for encryption, such as WhisperCore (https://whispersys.com) or Droid Crypt (http://tinyurl.com/hjlwb2v). Follow the device manufacturer's instructions for turning on encryption. It generally requires touching the Encrypt or Encrypt Tablet button in Settings. A strong PIN or password and automatic logoff after a set time are also important to keep the data encrypted. Like the iPhone, the device is automatically be encrypted when it is locked and decrypted when it is unlocked.

Google announced that starting with Android Lollipop (released at the end of 2014), Android encryption would automatically be enabled when a PIN, password, or swipe pattern is set. However, that was only implemented on limited Android devices. Google later announced that automatic encryption with a PIN, password, or swipe pattern will be included on new devices shipped with the latest version, Marshmallow. Again, it is important to follow the manufacturer's instructions when setting up encryption. Get help if you need it. First-time encryption takes some time when a device has already been in use, so make sure that the battery is fully charged before starting or better yet, have the charger connected.

Silent Circle (www.silentcircle.com) produces the Blackphone 2, a highly secure Android smartphone that includes peer to peer encrypted audio, video calling, and secure messaging. The secure audio, video calling, and secure messaging are also available as apps for iPhones and Android phones.

Open Whisper Systems (https://whispersystems.org) offers a free app/service that provides for iPhones and Androids encrypted voice and text communications, using their Signal product. Each person must be using the Signal application in order to maintain the end-to-end encrypted communication. It has been endorsed by Bruce Schneier, a leading security and cryptography expert, and Edward Snowden. We have heard that a number of attorneys are using its service.

The NSA has developed a high security version of Android called Security Enhanced (SE) Android. Some of its features are being incorporated by Google into the Android operating system. Android devices using Android SE and strong controls are reportedly being produced for the federal government for military and national security use.

Weaknesses have been reported in the encryption for both iOS and Android, so it is important to consider multiple levels of security. Despite some limitations, smartphones and tablets are more secure with encryption, and attorneys should be using it.

It is also important to make sure that secure methods are used for getting files on and off smartphones and tablets and for sharing files. There is substantial concern about the security of consumer services such as Dropbox (www.dropbox.com) and iCloud (www.icloud.com). Their terms of use provide limited protection and they control the encryption—so their employees can get access, and protection from unauthorized third parties depends on how well they protect the decryption keys. Use of alternatives such as business versions of Box (www.box.com) or SpiderOak (https://spideroak.com), using add-on

end user encryption like BoxCryptor (www.boxcryptor.com), Sookasa, (www.sookasa.com), Viivo (https://viivo.com), and Dell Data Protection | Cloud Edition (www.dell.com) with services like Dropbox provides stronger security because the end user controls the decryption keys. It should be noted that Dropbox has been adding security capability to its business offerings and may be a viable option after it has been fully implemented and evaluated.

6. Encryption of Portable and Mobile Devices: A Security No-Brainer

Encryption is particularly important for laptops, smartphones, tablets, and portable media because they can easily be lost or stolen. The *Verizon 2014 Data Breach Investigation Report*, which covers 2013, explains the risk and a solution to it—encryption—this way: [16]

> ***PHYSICAL THEFT AND LOSS—RECOMMENDED CONTROLS***
>
> The primary root cause of incidents in this pattern is carelessness of one degree or another. Accidents happen. People lose stuff. People steal stuff. And that's never going to change. But there are a few things you can do to mitigate that risk.
>
> ***Encrypt devices***
>
> Considering the high frequency of lost assets, **encryption is as close to a no-brainer solution as it gets for this incident pattern**. Sure, the asset is still missing, but at least it will save a lot of worry, embarrassment, and potential lawsuits by simply being able to say the information within it was protected.
>
> (Emphasis added.)

It's not just Verizon; this view is widely held by information security professionals and government agencies.[17] Encryption can protect all of the mobile technology used by attorneys, including smartphones, tablets, laptops, mobile devices and portable storage (e.g., external hard drives, USB drives, DVDs and CDs).

Encryption solutions for mobile devices are readily available, inexpensive, and generally easy to set up and use.

7. Wireless Networks

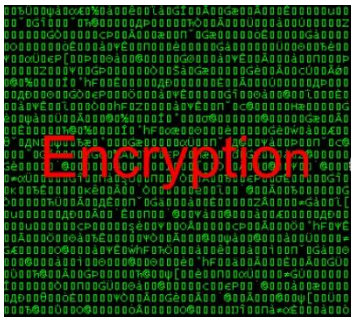
Communication via wireless connections needs to be secured as well in order to protect the transmission. Encrypting the wireless network will protect the data from being intercepted and viewed. There are many free "sniffer" applications that can be used to view the contents of unencrypted data streams. Essentially, there are three commonly available types of encryption schemes for your wireless network: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2 (second-generation WPA). These encryption methods can be used on all currently available wireless access points. WEP is very weak encryption and is fairly easy to crack. There are plenty of free tools available that can crack WEP in a matter of minutes. WEP should not be used in any wireless network because of its insecurity. WPA is a stronger form of encryption, but it has also been cracked. Therefore, WPA is not recommended

16 www.verizonenterprise.com/DBIR/2014.

17 E.g., US-CERT, the National Institute of Science and Technology (NIST), the Federal Communications Commission, and the Department of Health and Human Services have all recommended or required encryption on mobile devices to protect confidential information.

either. WPA2 is secure and should be the encryption method of choice for wireless networks. As with other forms of password management, the WPA2 pass phrase should be long and complex.

In addition to making sure that their wireless networks are secure, attorneys should ensure that third-party wireless networks that they use for client matters are protected by encryption. They should be protected by WPA2 as well and require a user name and password for access. This is particularly the case for public networks. Many security professionals and US-CERT (United States Computer Emergency Readiness Team) have recommended that public networks should not be used for confidential communications. If public networks are to be used, attorneys should obtain technical assurance that they are being securely used through protection such as a secure (https) connection to a trusted website or a virtual private network (VPN). A recent ethics opinion concluded that an attorney has an ethical duty to evaluate the security of a wireless network, home or public, *before* it is used for client communications and to take appropriate precautions in using it. California Formal Opinion No. 2010-179.



8. E-mail

Particularly important to attorneys is the confidentiality and integrity of e-mails. As discussed above, respected security professionals have for years compared e-mail to postcards—or to postcards written in pencil. They can be viewed or altered by third parties. While some ethics opinions have been incorrectly interpreted as concluding that e-mail encryption is never required, they do contain exceptions and qualifications. Some newer opinions provide that encryption may be required for at least some communications. In addition, ethics opinions set minimum requirements and do not address all of attorneys' duties to safeguard cli

For e-mail, the term *encryption* is generally used to mean both encryption and the authentication process that are used, in combination, to protect e-mail. Encryption protects the confidentiality of e-mail. Authentication identifies the sender of an e-mail and verifies its integrity.

Encryption is a process that translates a message into protected electronic code. The recipient (or anyone intercepting the message) must have a key to decrypt it and make it readable. Although it still takes some technical knowledge to set up, e-mail encryption is now easier to use than it once was.

Encryption generally uses a pair of keys to encrypt the e-mail. The sender uses the recipient's public key to encrypt the e-mail and any attachments. Because the public key only encrypts the e-mail, it does not matter that it is available to the public or to various senders. The recipient then uses his or her private key to decrypt the e-mail. It needs to be safeguarded because anyone who has access to the private key can use it for decryption.

The process is easy to use once the keys are set up in an e-mail program such as Outlook (www.microsoft.com). The most difficult process is getting the keys (digital IDs) and making the public key available to senders. Once it is set up in Outlook, the sender just has to click on the Message tab in the Options group and click the Encrypt Message Contents and Attachments button. At the recipient's end, the message will automatically be decrypted if his or her private key has been installed.

Digital authentication of e-mail also generally uses a key pair. The sender uses his or her private key to digitally sign the e-mail. The recipient then uses the sender's public key to verify the sender and integrity of the message. In Outlook, after installation of the private key, the sender clicks the Options tab in the Permission group and clicks Sign Message. After the sender's public key has been installed in the recipient's compatible e-mail program, the recipient will receive an automatic notice of verification of the sender and integrity.

For protection of confidentiality and authentication, the sender's and recipient's key pairs are used in combination. The sender uses both the Encrypt Message and Attachments command button (that uses the recipient's private key) and the Sign Message command (that uses the sender's private key). At the receiving end, the e-mail program automatically uses the recipient's private key to decrypt the messages and automatically uses the sender's public key to verify authenticity and integrity.

Again, the challenging part is obtaining key pairs, exchanging public keys, and setting them up in the e-mail program for encryption. Keys are available from commercial public key authorities such as Verisign (now part of Symantec; www.verisign.com). Public key authorities have online directories where their customers' public keys are available. The management and exchange of keys is a major reason why attorneys do not encrypt e-mail. Instead, they are more likely to use an encryption service that provides encrypted e-mail delivery without key exchange.

Another form of e-mail encryption is Transport Layer Security (TLS) encryption. It automatically encrypts e-mail between two e-mail gateways. If a law firm and client each have their own e-mail gateways, TLS can be used to encrypt automatically all e-mails between them. TLS encryption protects e-mails between e-mail gateways only. It does not protect e-mails within the sender's and recipient's networks and does not protect e-mail that is misaddressed or forwarded through other e-mail gateways.

Secure e-mail is also available from managed messaging service providers such as Zixcorp (www.zixcorp.com), Mimecast (www.mimecast.com), and DataMotion (www.datamotion.com). They provide e-mail encryption without the complexity of setting up and exchanging keys.

As an alternative to e-mail, confidential information can be exchanged by using secure file sharing and transfer options such Biscom (www.biscom.com) or Accellion (www.accellion.com) or by using add-on encryption, e.g., BoxCryptor (www.boxcryptor.com/en), Dell Data Protection|Cloud Edition (www.dell.com), Sookasa, (www.sookasa.com), or Viivo (https://viivo.com) with Dropbox or another cloud vendor).

Another alternative to encryption of e-mail is to give confidential information a basic level of protection by putting it in a password-protected attachment rather than in the body of the e-mail. File password protection in some software, such as current versions of Microsoft Office, Adobe Acrobat (www.adobe.com), and WinZip (www.winzip.com), uses encryption to provide security. It encrypts only the document and not the e-mail, so the confidential information should be limited to the attachment. It is generally easier to use than complete encryption of e-mail and attachments. However, the protection

can be limited by the use of weak passwords that are easy to break or "crack." In addition, it should be obvious not to include the password for the attachment in the body of the e-mail message.

Electronic communications have now reached the point that most attorneys should have encryption available for use in appropriate circumstances. In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality of electronic communications is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.

9. Securing Documents

Most attorneys already have encryption tools for basic protection of documents. They're free and easy to use. File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip, uses encryption to protect security. As discussed above, New Jersey Ethics Opinion 701, published in 2006, states that attorneys should password protect confidential documents sent over the Internet. With these modern programs, this means encrypting them.

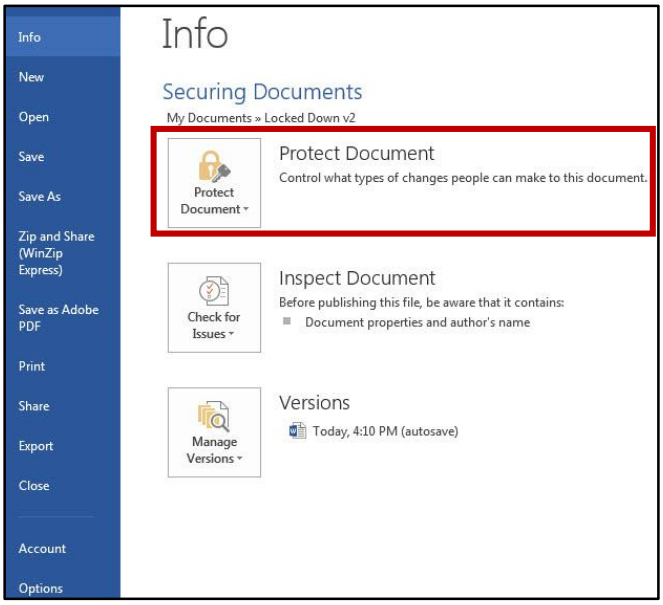
It should be noted that password protection of documents with these kinds of programs provides basic, but limited protection. There are tools available to crack passwords and enable brute force access to files. Depending on the strength of your password or passphrase, this could take minutes or years. The more effective products cost thousands of dollars. The message is, don't consider your documents to be 100% secured even if strong passwords are used. However, for all practical purposes, a strong password is sufficient protection to restrict access to the data.

Microsoft Word is a good example of how easy encryption with passwords can be. Ever since Word XP (also known as Word 2002), applying a password to your document also encrypts it. There are two levels of security that can be set for the document. One level allows a user to open the file, and the other level allows for editing of the document itself. We'll only discuss securing documents using Word 2007 and above. Office 2003 and earlier is out of support and no longer receiving any updates, including security updates That means that you may be violating your ethical duties if you continue to use it since the software is vulnerable to attack and compromise of client confidential information.

The procedure for Word 2007 is a simple task. Click on the Office button and then put your mouse over the Prepare choice. This will open up additional selections to the right of Prepare. Select the Encrypt Document option to bring up a password dialog box. Make sure that you use a strong password as we've recommended throughout this paper. Click on OK and you will be asked to confirm the password. This password encrypts the document and will be required to open the file in the future. Don't forget the password; if you do, you won't be able to recover it or the contents of the document.

Encrypting a Word 2010 document is a little easier, primarily since the Ribbon was redesigned with the removal of the Office button. Select File and then the Protect Document button in the Permissions section. Select Encrypt with Password to launch the password dialog box. Enter a strong password and click OK. You will be asked to confirm the password, which will encrypt the document.

The process for Word 2013 and Word 2016 is very similar to Word 2010. Select the File tab and the Info selection in the left hand menu structure. Click on the Protect Document button in the Securing Documents section. Word 2016 removed the "Securing Documents" and folder location above the Protect Document button. Once you click on the Protect Document button, select Encrypt with Password. Like Word 2010, you will be prompted to enter a password and to confirm the password that will be used to encrypt the document.



It's this easy. An attorney who wants to send a confidential document to a client can password protect (encrypt) the document, attach it to an e-mail, and communicate the password in a secure way – by phone or text or other communication channel different from e-mail. (Certainly don't include the password in the same e-mail as the document.) The document then has a basic level of protection if it's sent to the wrong recipient or intercepted. It's not as strong as fully encrypted e-mail (including attachments) or secure file transfer, but much better than no protection.
Password protecting (encrypting) files Acrobat and WinZip uses similar steps and is just as easy.

10.Conclusion

Attorneys have ethical and common law duties to protect information relating to clients and often also have contractual and regulatory duties. The Ethics 20/20 updates to ABA Model Rules 1.1 and 1.6 made explicit attorneys' duty to take competent and reasonable measures to safeguard information relating to clients. Encryption is an important consideration in addressing these duties.

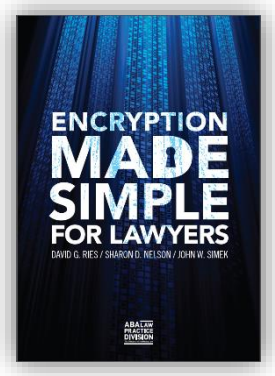
Encryption is now a generally accepted practice in information security for protection of confidential data – both in transmission and storage. Attorneys should understand encryption and use it in appropriate situations. All attorneys should use encryption on laptops, portable storage media, smartphones, and tablets that contain information relating to clients and other confidential data. They should make sure that transmissions over wired and wireless networks, remote access, and document exchange are secure. Attorneys should have encryption available for e-mail or secure file transfer and use it when appropriate. There are now easy to use (after setup) and inexpensive (sometimes free) encryption solutions that are readily available.

David G. Ries (dries@clarkhill.com) is a member of Clark Hill, PLC, in Pittsburgh, Pennsylvania. John W. Simek (jsimek@senseient.com) is Vice President of Sensei Enterprises, Inc., a legal technology, information security, and digital forensics firm in Fairfax, Virginia. They are co-authors, with Sharon D. Nelson, of *Encryption Made Simple for Lawyers* (American Bar Association 2015) and *Locked Down:*

Information Security for Attorneys (American Bar Association 2012, second edition scheduled for March 2016 publication).

An Encryption Quick Start Action Plan

This Quick Start Action Plan is from *Encryption Made Simple for Lawyers* (American Bar Association 2015). References to Chapters are to the book.



An American Bar Association resolution adopted in August 2014 *"encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected*." It covers attorneys and law firms, as well as other businesses and enterprises. An appropriate information security or cybersecurity program is an essential part of compliance with attorneys' duty under ABA Model Rule 1.6(c) to employ "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Encryption of data is a critical component of an appropriate information security or cybersecurity program. (Chapters 2 and 3)

This Quick Start Action Plan outlines the steps that attorneys can take to implement encryption – **starting now**.

1. **Start with the basics for encryption that you are using now or implementing in the future.** (Chapter 5)

    a. **If you need help in implementing encryption, find someone who is qualified to assist you.**

    b. **Protect encrypted data with strong authentication.**
    In many implementations of encryption, access to the decryption key is protected by the user's password or passphrase. Make sure that you have strong passwords or passphrases for encryption you are currently using or you plan to implement in the future.

    c. **Back up data.**
    Like other areas of technology, there can be technical failures with encryption hardware and software. Keep a secure backup of encrypted data, a step that should always be done, even for data that is not encrypted.

    d. **Back up the recovery keys.**
    In some implementations of encryption, a user can back up a recovery key that may make encrypted data recoverable if a user forgets a password or there is a technology problem. Back up the recovery key in a secure place. In mid-sized and larger firms, recovery keys should be managed by IT staff.

2. **Start with the "no-brainer" encryption solutions – encryption of laptops, smartphones, tablets, and portable drives.** (Chapters 5, 6 and 7)
    The Verizon 2014 Data Breach Investigation Report notes that "encryption is as close to a no-brainer solution as it gets" to protect confidential data on lost or stolen laptops and mobile

devices. It's not just Verizon, this view is widely held by information security professionals and government agencies. Review the devices that you and your firm are using – laptops, smartphones, tablets, and portable drives - and make plans to encrypt them as soon as reasonably possible if they are not already encrypted. With many of them, it's just a matter of turning encryption on. Consider encryption and enable it when you add new devices.

3. **Protect confidential documents with encryption – <u>a solution you already have</u>.** (Chapter 11)
   Confidential documents transmitted electronically or by e-mail should be protected by encryption. Current versions of Microsoft Office, Adobe Acrobat and WinZip encrypt documents when password protection is used. New Jersey Ethics Opinion 701 (April 2006 - over eight years ago) advised attorneys to password protect documents [encrypt them] when they are sent over the Internet. (Chapter 2.) While this form of encryption may not be as secure as some of the other solutions discussed in the book, it is much more secure than no encryption and is immediately available to most attorneys.

4. **Use secure network connections.** (Chapter 8)
   Confidential data that is transmitted outside of a secure network should be protected. This requires secure connections between networks and over the Internet. Review the various network connections that you and your firm use and make sure that they are secure. For the Internet, you should use https:// or virtual private networks as a minimum.

5. **Secure your wireless networks.** (Chapter 8.)
   Make sure that your law office wireless network and home networks used for client data are protected by WPA2 (Wi-Fi Protected Access 2) encryption and are securely configured. If you are using an older wireless access device that does not support WPA2, replace it.

6. **Be careful on public networks.** (Chapter 8)
   Make sure that you can use a public network securely for confidential data **before** you use it, or avoid using it. Use only secure connections – https:// or a virtual private network.

7. **Implement an encrypted e-mail solution.** (Chapter 9)
   It has now reached the point where most or all attorneys should have the ability to use encrypted e-mail, where appropriate, for confidential communications. A basic level of protection can be provided by putting the confidential communication in a password protected/encrypted attachment. There are now a number of easy to use, inexpensive options that are available for securing e-mail, including ones for solos and small firms.

8. **Use encryption in the cloud.** (Chapter 10)
   Encryption controlled by the end-user should be the default for confidential data stored in the cloud. End-user controlled encryption should be required for attorneys unless the attorney makes an informed decision that the data is not sensitive enough to require this level of protection or that the cloud service provider will implement and maintain sufficient security controls without end-user controlled encryption. For attorneys, this requires the analysis required by the ethics rules and opinions discussed in Chapter 2, including competent and reasonable measures to safeguard information relating to clients, due diligence concerning service providers, and requiring service providers to safeguard data in accordance with attorneys' confidentiality obligations.