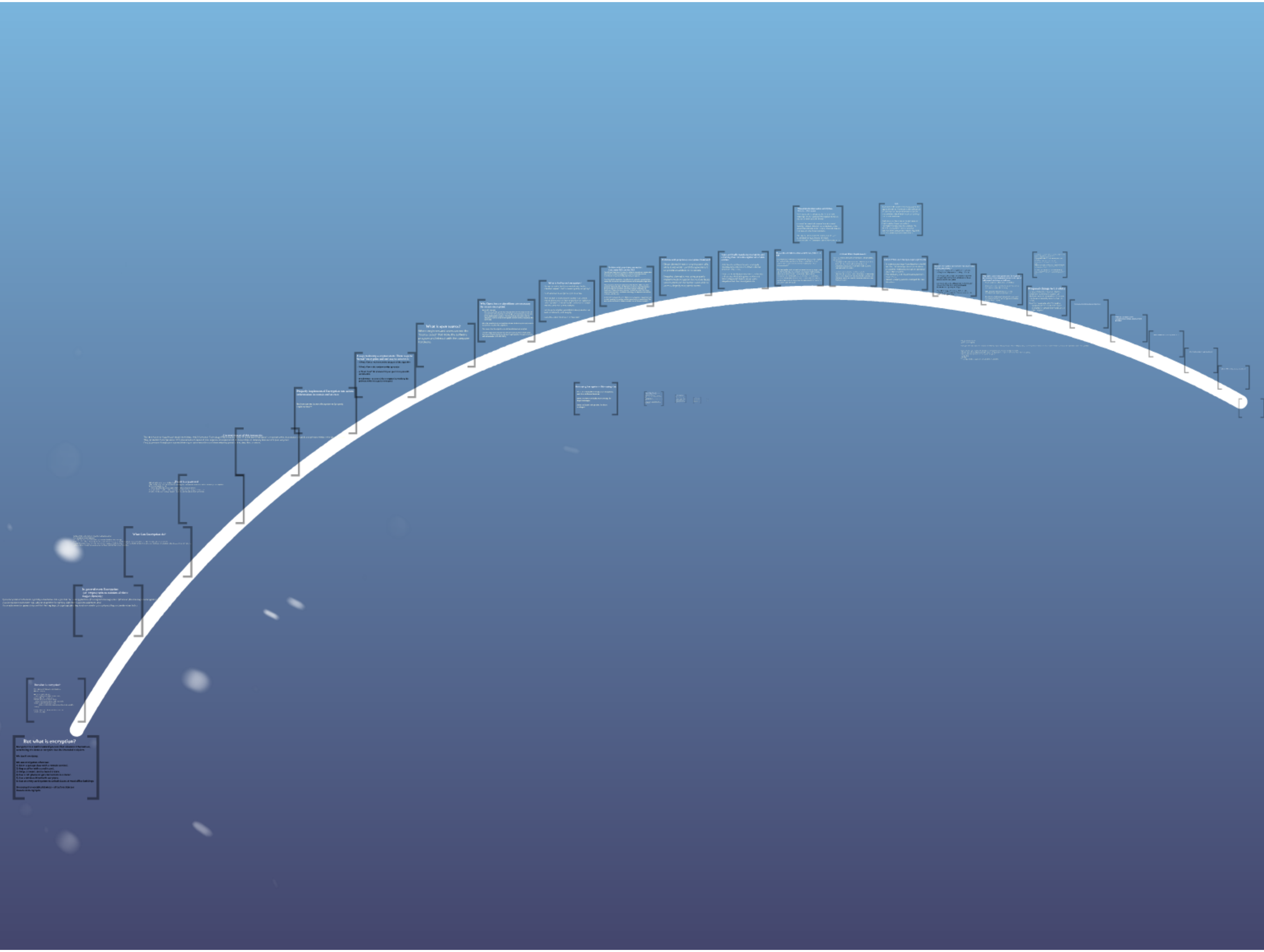
But what is encryption?
What Can Encryption do?
What is open source?

But what is encryption?

Encryption is a mathematical process that obscures information, scrambling the data to everyone but the intended recipient.

We use it everyday.

We use encryption when we:
1) Enter a garage door with a remote control.
2) Buy a coffee with a credit card.
3) Swipe a smart card to board a train.
4) Use a cell phone to get connection to a tower.
5) Use a wireless Bluetooth ear piece.
6) Use an entry card system to unlock doors at most office buildings

Six encryption-enabled devices—all before 9:00 am
Dozens more by 5pm.

But saying Encryption is like saying Car.

There are many different types of encryption, each for a different function.

Some are slower and take more energy, for larger messages,

Some are faster and quicker, for short messages.

Every Encryption (or crypto) system consists of three major elements:

1) an encryption mechanism,
typically a mathematical algorithm for turning plaintext (the original message) into ciphertext (the message in encrypted form);

2) a decryption mechanism,
typically an algorithm for turning ciphertext back into plaintext; and

3) a mechanism for generating and distributing keys.
(A cryptographic key function similarly to a physical key or combination lock.)

What Can Encryption do?

Confidentiality, Authentication, Integrity, and Nonrepudiation

- **Confidentiality: only the intended message recipient should read the message.**
- **Authentication: It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.**
- **Integrity: It should be possible for the receiver of a message to verify that it has not been modified in transit.**
- **Nonrepudiation: A sender should not be able to falsely deny later that he sent a message.**

Email is a postcard,
Encryption puts your email in an envelope.

Unfortunately, very little of the information technology we use in our offices has the security properties encryption provides.

The clearest example is email:

1) Email is not confidential; it is a postcard when it travels across the network. A domestic network path can be international depending on electricity rates.

2) Normal Email lacks authentication, is it simple to send a message acting as someone else.

3) Normal email lacks message integrity, important elements could be modified in transit.

Current impact of this 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.

- 67 percent of IT Professionals self-reported their organization experienced the loss or theft of company data over the past two years
- Only 22 percent of employees reported their organization was able to tell them what happened to lost, data, files, or emails.

Why open source encryption must be required for attorney client communications in the age of cyberattack and mass surveillance

- The profession as a whole is losing client trust.
- International structure of the internet. (Domestic email can travel internationally for routing)
- Multiple governments are attempting "mass surveillance" of all internet communication.
- International clients don't trust domestic government assurances based on “citizen” categories and attorney client privilege category

Properly implemented Encryption can secure information in transit and at rest:

But how can we be sure the system is “properly implemented”?

4 ways to destroy a cryptosystem: Three ways to “break” encryption and one way to subvert it:

- 1) Find a flaw or weakness in the structure of the algorithm
- 2) Find a flaw in the random number generator
- 3) "Brute force" the password/key (ie. guess every possible combination)
- 4) Subversion: Go around the encryption by watching the plaintext while it is typed or encrypted.

What is open source?

Where engineers and users can see the “source codes” that make the software program and interact with the computer hardware.

Why Open Source algorithms are necessary for secure encryption:

- **Kerchoff's Principle**

  The security of the system has to be based on the assumption that the attacker has full knowledge of the design and implementation details of the cryptographic system. The only missing information for the attacker is a short, easily exchangeable random number sequence, the secret key

- **All of the security in these algorithms is based in the key (or keys); none is based in the details of the algorithm.**

- **This means that the algorithm should be published and analyzed.**

- **The best algorithms we have are the ones that have been made public, have been attacked by the world's best cryptographers for years, and are still unbreakable. (PGP, OTR, ZRTP)**

What is End-to-end encryption?

- Encryption system built to be readable only by the intended recipient, and the receiving party decrypting it
- No involvement in encryption by third parties.
- The intention of end-to-end encryption is to prevent intermediaries, such as Internet providers or application service providers, from being able to discover or tamper with the content of communications.
- End-to-end encryption generally includes protections of both confidentiality and integrity.
- Sometime called “Client-side” or “User-side”

Problem with proprietary encryption: Case study RSA and the NSA

- The NSA put “back doors” (a term for a flaw in the software construction that allows surveillance programs to access supposedly secured information) in Dual_EC_DRBG proprietary encryption.

- The NSA did this by paying $10 million to an encryption manufacturer, named RSA, to weaken the math that secured its encryption algorithm.

- The companies that have implemented the Dual_EC_DRBG into their products include Blackberry, Microsoft, Certicom, RSA, Cisco, Juniper Networks, McAfee, Symantec, Samsung, Lancope, SafeLogic, GE Healthcare, Thales eSecurity, Panzura, Catbird Networks, ARX, Kony, CoCo Communications, Riverbed Technology, The OpenSSL Foundation, Certicom, and Mocana.

- In 2014 NIST removed Dual_EC_DRBG as a cryptographic algorithm from its draft guidance on random number generators, recommending "that current users of Dual_EC_DRBG transition" to a different algorithm.

Problems with proprietary encryption: Continued

- Skype claimed it was encrypting user calls, while it was working with the government to provide a backdoor to its service.

- Snapchat claimed it was using properly implemented encryption, but its data bases were hacked and the hackers were able to access allegedly encrypted content.

States are legally mandating encryption, and enforcing those mandates against out of state entities:

- Both Nevada and Massachusetts have legally mandated encryption as part of their consumer protection regulations.

- In July 2014, the MA Attorney General, enforced a civil penalty of $150,000 against the Women & Infant's Hospital of Rhode Island to resolve allegations that it lost unencrypted data.

Massachusetts information security law, M.G.L. c. 93H

- 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 a written organization wide 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."

Massachusetts information security law, M.G.L. c. 93H (cont)

- 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.

Current Ethics Requirements:

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."

Cont.

- 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.

Current Ethics don't live up to legal requirements

- In order to avoid significant fees from the MA Att. Gen. NY Attorneys must screen clients and parties involved to encrypt the personal data of MA residents.
- This confusing and requires two systems in most offices.
- Doesn't properly protect privileged for non-MA actors.

But isn't encryption too expensive for small firms or solo practitioners?

- Open source end-to-end encryption is free and costs nothing to use. Only expense is training and setup.

- Free encryption Phone apps, like Redphone, (Android) and Signal (Iphone) have over 500,000 users and use open source ZRTP encryption

- Open source phone to desktop programs, like Telegram, have over 50 million active users and allow for document exchange of up to 1.5 gigs.

- Tor, OTR, Veracrypt, Tails OS and PGP are all free standards used by hundreds of thousands which can be used for office applications.

Proposed change to 1.6 ethics

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Redefine “reasonable effort” to require:

- “provision of end-to-end open source encryption for private information and at client request.”

Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to:
(i) the sensitivity of the information;
(ii) the likelihood of disclosure if additional safeguards are not employed;
(iii) the cost of employing additional safeguards;
(iv) the difficulty of implementing the safeguards;
and
(v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or 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 forgo security measures that would otherwise be required by this Rule.