The Legal Ethics of Cybersecurity

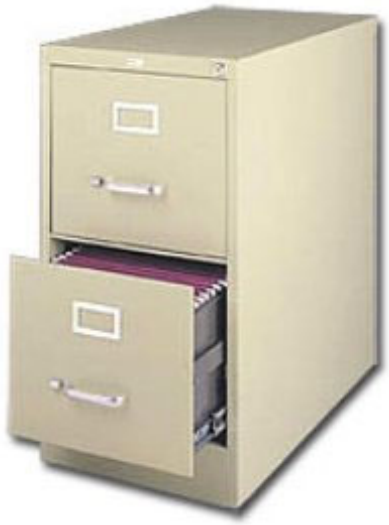
(While we're waiting to get started, text Suffolk to 22333)

Andrew Perlman

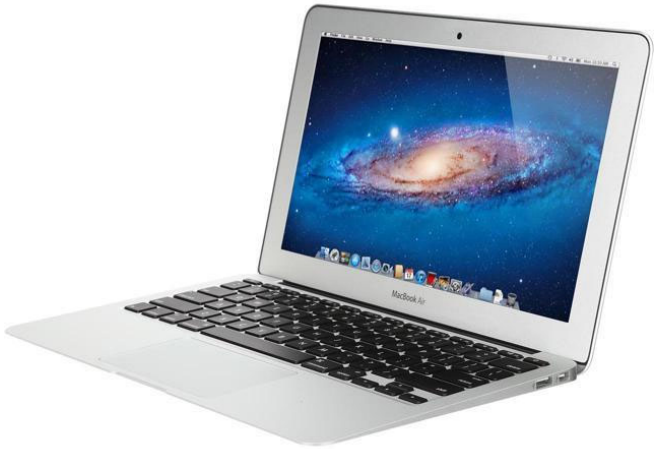
Dean & Professor of Law

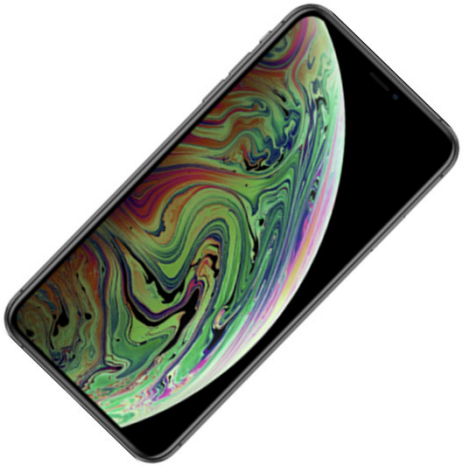
SUFFOLK UNIVERSITY BOSTON | LAW SCHOOL

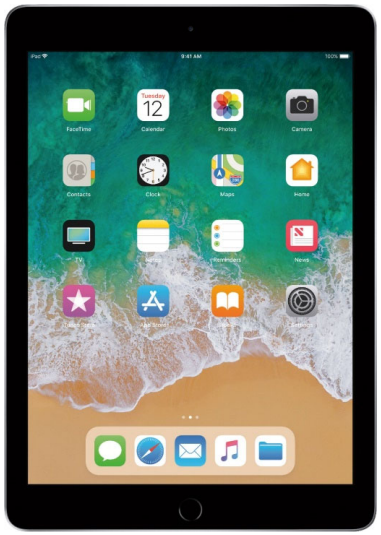
Protecting Client Information in the Past

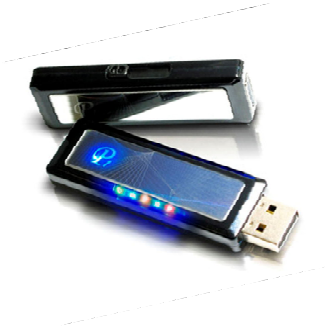


Protecting Digital Information Today









Hypo on Technology and Confidentiality

A lawyer keeps confidential client information on a laptop, smartphone, flash drive, and in the "cloud." What steps must the lawyer take to satisfy her ethical obligations to protect the confidential information?

- Answer under the old (pre-August 2012) Model Rules?
- Under the new version of the Model Rules (now adopted in the vast majority of states)?

Technology and Confidentiality

The newly adopted changes:

- clarify that lawyers should take reasonable precautions to protect client confidences from inadvertent disclosure as well as unauthorized access or disclosure (Model Rule 1.6)

- identify the factors that lawyers should consider when determining whether they have taken reasonable precautions (Model Rule 1.6)

Factors to Determine the Reasonableness of a Lawyer's Efforts

- Sensitivity of information
- Likelihood of disclosure without safeguards
- Cost of additional safeguards
- Difficulty of implementing safeguards
- Extent to which the safeguards adversely affect the lawyer's ability to represent clients

A hypo on cloud computing…

The "answer"

- It depends.
- Ethics opinions generally conclude that it is ***ethically permissible to use the cloud***, as long as lawyers take ***reasonable precautions*** to protect the information. What counts as reasonable continues to evolve.

Two hypos about email….

The "answer"

- ABA Formal Opinion 477 (2017)
  - "The use of unencrypted routine email generally remains an acceptable method of lawyer-client communication."
  - "However, … it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable."
  - The Opinion goes on to offer a number of considerations.

And finally, a hypo about a data breach…

Formal Opinion 483
October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Takeaway Messages

- The rules of professional conduct address cybersecurity issues in general terms and offer a variety of factors to consider.
- The application of those factors to specific situations could lead to a finding that a lawyer has violated the rules.
- Conduct that might have been considered ethically permissible 5 years ago might not be ethically permissible today.