ARMORTEXT

Communications and Mobile Security for Legal Professionals

Excerpts from the ABA Guidance on “Ethical & Risk Management Issues for Law Firms”

www.ArmorText.com

While law firms have not traditionally seen themselves as attractive targets for state-sponsored hacks and industrial espionage, they are now prime targets and should take defensive measures to protect their reputations, clients and profits.

The American Bar Association, which released its ABA Guidance on "Ethical & Risk Management Issues for Law Firms" is clear about the responsibilities of lawyers when it comes to ensuring privacy and security in their communications with clients.

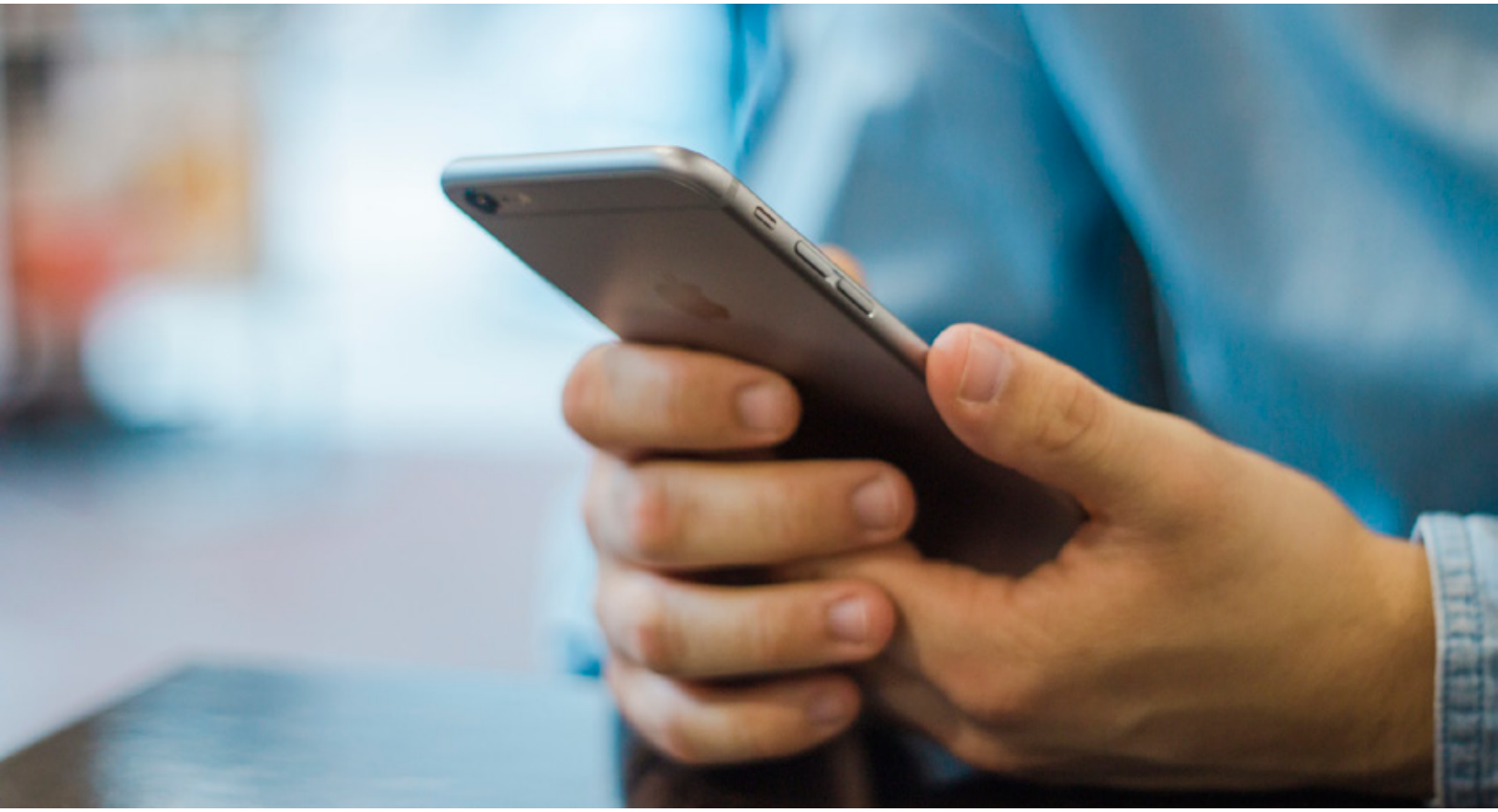
Here are some excerpts:

> ***The 2012 amendment to Model Rule 1.1 precludes a lawyer from pleading ignorance of the risks associated with technology. Lawyers are expected to have at least a basic understanding of the risks associated with the technologies they use and the protections available to mitigate those risks. This obviously includes mobile devices used by lawyers.***

(Section III: A LAWYER'S DUTY OF COMPETENCE REQUIRES KNOWING THE RISKS AND BENEFITS OF TECHNOLOGY)

> ***The duty of competence also requires that lawyers be aware of the benefits and risks of emerging technologies that can be used to deliver legal services and how advances in existing technologies can impact the security of information in their possession.***

(Section III: A LAWYER'S DUTY OF COMPETENCE REQUIRES KNOWING THE RISKS AND BENEFITS OF TECHNOLOGY)

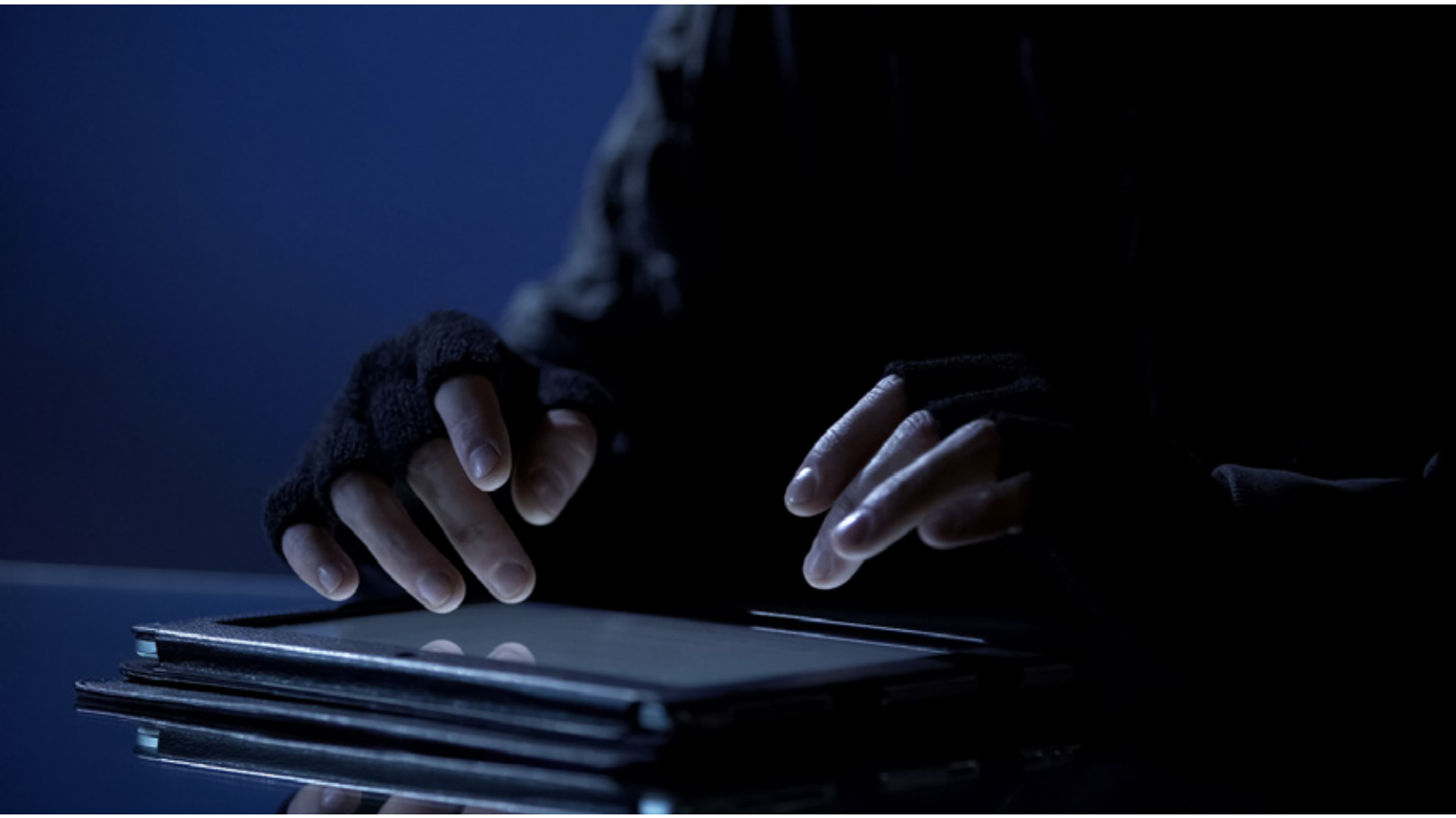


> ***Last year, it was estimated that 3.1 million smart phones were stolen in the United States and another 1.4 million phones were lost and never recovered. All too often, these devices are protected by weak passwords, or a four-digit PIN that can be "cracked" by a cyber-criminal's brute force attack on the device. A poorly secured mobile device can result in the loss of confidential client or firm information and trigger another risk stemming from a statutory or ethical obligation to report a security incident or data breach to a client or third parties whose information was placed at risk.***

(Section IV: THE RISKS ASSOCIATED WITH MOBILE DEVICES)

Lawyers are obligated to take 'reasonable measures' to safeguard 'the integrity and security' of their electronic files. Among other things, this obligation requires that lawyers take 'reasonable steps' to ensure that 'only authorized individuals have access to the electronic files' and to ensure they 'are secure from outside intrusion.' Rule 1.6(c) requires a lawyer to 'make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.'

(Section V: THE ETHICAL DUTY TO SAFEGUARD AGAINST TECHNOLOGY-BASED RISKS)



> ***A lawyer's duty to safeguard information under its control cannot be transferred or delegated to a third party…Yet how many lawyers have considered whether their use of cloud-based applications or web-based mail accounts on their mobile devices trigger these issues? And how many lawyers have checked Google's terms of service for instance, and evaluated the potential impact of those service terms on the duty to maintain the confidentiality and security of client information?***

(Section VI: DUTY TO HAVE MEASURES REASONABLY ASSURING THAT LAWYERS ARE CONFORMING TO PROFESSIONAL CONDUCT RULES AND THE CONDUCT OF NON-LAWYER ASSISTANTS IS COMPATIBLE WITH LAWYERS PROFESSIONAL OBLIGATIONS)

> ***Given the increasing importance of encryption to data security, lawyers should inquire if the cloud provider encrypts information before it is stored in the cloud, if the provider has a process through which client information can be encrypted or if the provider will assist the lawyer to encrypt information before it is stored in the cloud.***

(Section VI(A): Cloud Computing and Cloud Storage Ethical Issues Arising From Mobile Technology)

ArmorText is the only unified communications offering for law firms that simultaneously addresses security, end-user experience, enterprise governance, and retention & review needs. It surpasses the Standards for Reasonable Care Recommendations issued by the American Bar Association, Connecticut State Bar, and Texas Disciplinary Rules of Professional Conduct 6482.

Encrypted and Secure

Full featured and easy to use

Cost effective

Surpasses ABA Standards