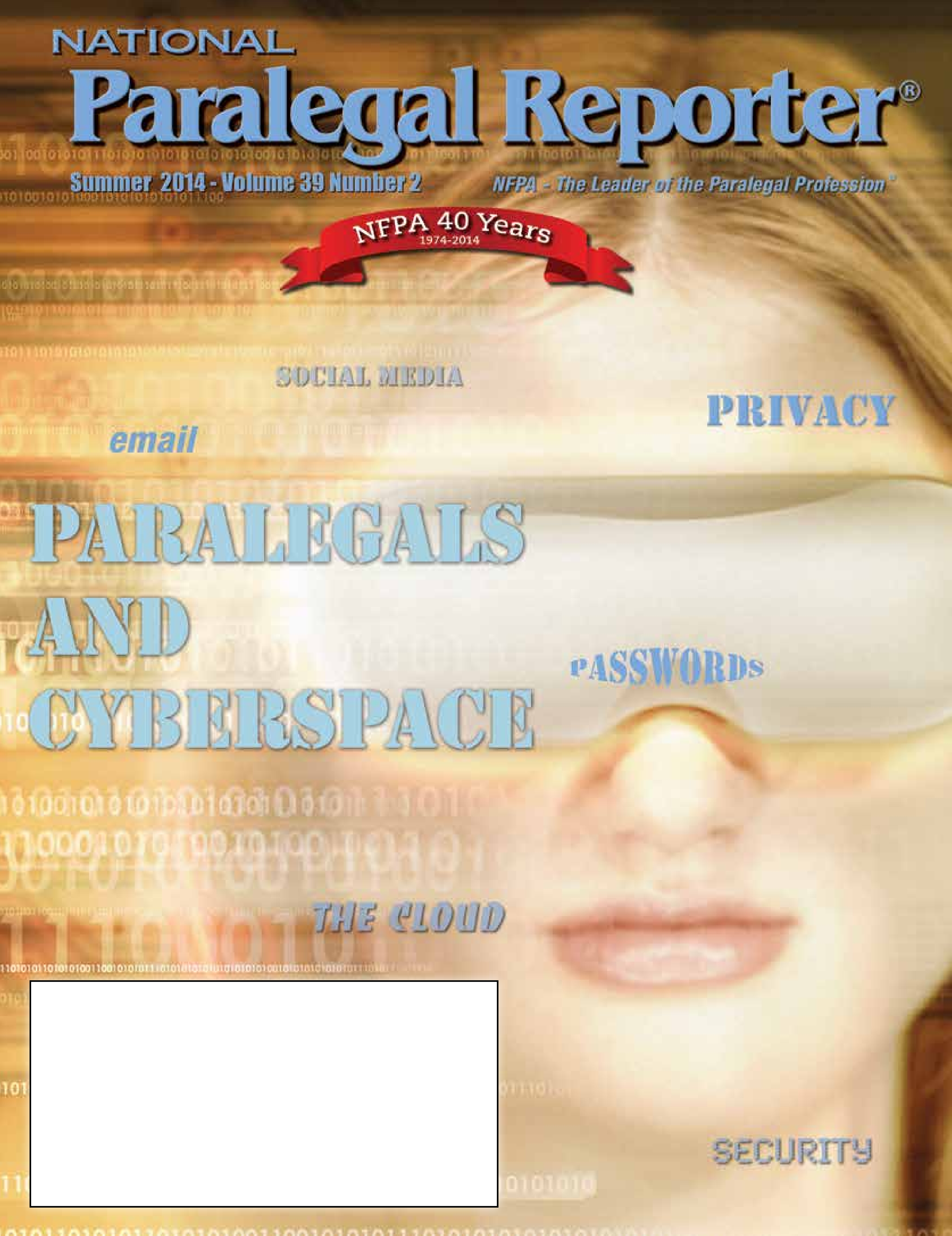
NATIONAL Paralegal Reporter®

Summer 2014 - Volume 39 Number 2

NFPA - The Leader of the Paralegal Profession®

NFPA 40 Years
1974-2014



SOCIAL MEDIA

PRIVACY

email

PARALEGALS AND CYBERSPACE

PASSWORDS

THE CLOUD

SECURITY

Minding 'The Cloud'

BY PAMELA J. STARR, CBA, J.S.M.

It takes a firm grasp on technology for paralegals to excel at their jobs. Our feet are firmly planted in the 'cloud', as the Internet, combined with our devices, apps, and software, renders us more productive, efficient, accessible, and vulnerable.

What is this 'cloud'? It is not some ethereal or nebulous construct that exists somewhere in the stratosphere, but is "a known road and location that data travels to and on and *does not mean that data is floating out in space unprotected and unobtainable*."[1] (emphasis added) For the uninitiated, the terms 'cloud' and 'cloud computing' originally referred to the visual devices programmers created to describe the complex network of systems involved in data transfer and storage in cyberspace. These web-based services increase productivity by allowing users to store and retrieve data that has been centrally stored on an outside server, i.e. web-based email, social media, online banking, e-commerce, and more.

Technology provides the tools for legal professionals to be more autonomous and produce exemplary work, anywhere and anytime. Attorneys and paralegals use cloud-based productivity applications to telecommute and work remotely. Files stored offsite can be viewed and edited in real time, by several users, from any Internet-connected device, and meetings, CLEs, and hearings are often conducted virtually. Whether working in a traditional workspace, or minding the cloud, lawyers, paralegals, and legal service providers are bound by the same legal and ethical constraints as their brick and mortar counterparts.

The Intersection of Technology and Ethics

With all these tools and advances, we find ourselves at the very busy intersection of technology and ethics. Not only does technology make it possible to work virtually from practically anywhere, it has also made it easier to inadvertently cross ethical lines.

We access the Internet anywhere and everywhere — from our homes, work, school, and even in-flight. Visualize every computer, laptop, tablet, cell phone, application, and other Internet portal as a window into your life. (They call them 'windows' for a reason.) Every window in your home has, at the very least, a reliable locking mechanism; most have some sort of covering — a pull-down shade, blinds, or even black-out curtains — to protect your privacy from the prying eyes of neighbors and passers-by. Our digital 'windows' require similar protection to protect personal information from interception by fellow travelers on the "interwebs."

So what does this mean for us as paralegals? Think about Snowden and the NSA, hacker attacks on retailers, and recent denial-of-service attacks on the CM/ECF system. Now consider the nature of the information transmitted from client to attorney, attorney to paralegal, and so on. Paralegals often have access to clients' personal information: credit reports, Social Security numbers, and accounting, financial and medical records, as well as other forms of protected information. Whether the information resides on a device or in the cloud, we are ethically bound to ensure that confidentiality, privacy, and security policies and protocols are established and enforced.

Confidentiality

In August 2011, the ABA Standing Committee on Ethics and Professional Responsibility published its opinion on the "*Duty to Protect the Confidentiality of E-mail Communications with One's Client*." Among other things, the opinion addresses concerns as to the risk of third party access to any online communication:

> A lawyer sending or receiving substantive communications with a client via email *or other electronic means* ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by email, the lawyer *must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications*. If so, the lawyer must take reasonable care to protect the confidentiality of the communications *by giving appropriately tailored advice to the client.*[2] (emphasis added)

Obviously, this legal and ethical obligation to protect client data applies to paralegals in addition to the attorneys to whom the opinion was originally directed.

Privacy

Unless you choose to return to the time of "stone knives and bear skins,"[3] you must accept that personal information is no longer sacrosanct. Legally speaking, Personally Identifiable Information (PII) is:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[4]

As soon as you connect to the Internet, your personal information becomes vulnerable. Whether you are reading or sending email, participating in a listserv, posting to Twitter, updating Facebook, submitting a blog post, commenting on LinkedIn, making online purchases and payments, checking your bank and credit card accounts, IM-ing, chatting, Skyping, making VoIP calls, clicking a link, or sending information from your cellphone or tablet, you have flung the (previously mentioned) window wide open.

We, as a society and professionals, have become far too complacent about sharing information. We liberally supply our names, phone numbers, email addresses, and more on online forms. All it takes is a simple click of the mouse to release that information, irretrievably, into the ether and potentially into disreputable hands. Our easygoing attitude toward sharing information combined with the trend toward BYOD (bring your own device) is a recipe for disaster.

Security

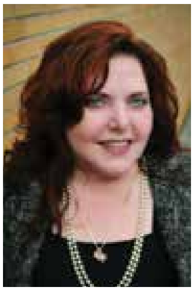
Every online activity has the potential to reveal confidential information. With so many paralegals working virtually and remotely, security is crucial. Not only do you need to know the physical location of your devices and servers, as well as the type of Internet connection being used, but it is also essential to implement and follow safety protocols. To quote Ben Schorr, author of *Office for Lawyers* (**www.officeforlawyers.com**), "security is a process, not a product."

Getting Started

So, what should your process be? To start:

- Whenever possible, avoid public hotspots and use a secure Internet connection to reduce exposure to eavesdropping, piggy-backing, and hacking. When a secure connection is unavailable, use some form of Virtual Private Network (VPN) software to encrypt the signal.
- Use (and regularly change) complicated passwords/passphrases. Short, simple passwords are vulnerable to dictionary and brute force attacks. The best passwords/passphrases contain 12 or more characters, and incorporate upper and lower case letters, symbols, spaces, and punctuation.
- Install and enable VPNs, firewalls, and programs to detect and remove adware, spyware, malware, viruses, browser hijackers, cookies, data miners, temporary files, and virus remnants.
- Read Privacy Statements and Terms of Service for everything — website access, downloads, web hosting, cloud service providers.
- Confirm where the servers are located and where the data is stored – servers and data stored outside the U.S. are subject to the laws of the jurisdiction in which they are physically located.
- Determine whether secure technology is used to protect your information: what information is collected and for what purpose; to whom is access to the information permitted; and how is the information backed up?
- Look for sites that implement Secure Sockets Layer (SSL), Transport Layer Security (TLS) protocols, and HTTPS (Hypertext Transfer Protocol Secure) encryption.

Remember, once information has been committed to the interwebs, it is out there forever. Nothing on the Internet is ever truly deleted. Information is shared, stored, and cached. Safe surfing involves keeping your windows locked and covered.



Pamela J. Starr launched StarrParalegals in 2008 to provide 21st century paralegal support to attorneys in Bankruptcy & Creditors' Rights, Commercial Transactions, UCC, and all things ECF. In her role as Paralegal Extraordinaire, she helps attorneys throughout the US make their "billable dollar worth every penny."© Pamela, a former Georgia Association of Paralegals' Membership Vice President, serves on NFPA's Ethics Board, blogs as her alter ego, 'Pamela the Paralegal', provides Career Mitigation© services to transitioning professionals at 'Sessions with a Starr' and attends grad school. She can be reached at pjstarr@starr-paralegals.com.

[1] Stephanie L. Kimbro, Virtual Law Practice: How to Deliver Legal Services Online (ABA, Law Practice Management Section. 2010).

[2] ABA Standing Committee on Ethics and Professional Responsibility, *Duty To Protect The Confidentiality of E-Mail Communications with One's Client*, Formal Opinion 11-459 (2011).

[3] *Star Trek — The City on the Edge of Forever* (Desilu Productions, April 6, 1967).

[4] E. McCallisterm, NIST Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information* (PII) (2010-05-12, 2010).