Ethics: Protect Your Electronic Contact List from Prying Eyes

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Introduction to an Ethical Problem Most Attorneys Don't Know About

In April of 2022, a headline caught our attention. It referenced a new legal ethics opinion issued by the New York State Bar Association's Committee on Professional Ethics. Opinion 1240 has this digest statement: "If 'contacts' on a lawyer's smartphone include any client whose identity or other information is confidential under Rule 1.6, then the lawyer may not consent to share contacts with a smartphone app unless the lawyer concludes that no human being will view that confidential information, and that the information will not be sold or transferred to additional third parties, without the client's consent."

So . . . what client information do you have in your Contacts – and how many apps have you granted the power to access your Contacts? If you are clueless about whether you have granted this access to various apps, you are part of a very large club.

What Do You Actually Store in Your Contacts?

All lawyers likely have the client's name, office and cell number, email and physical address and job title. But many keep other information in the Notes field of Outlook, including such things as nicknames, anniversaries, birthdays, spouse's name, names of children, pet names. etc. If you click on "Details" in the ribbon, you have a specific form for entering certain details, but most lawyers, in our experience, simply dump the information into the Notes field when they create a new contact.

Because we do digital forensics, we can tell you that there is often a lot of information in the Notes field, including passwords, social security numbers, building access codes and a lot of other private information which the attorney wants readily at hand.

Many lawyers have no clue that apps can potentially see all that information if you grant them access. A quick search on Google shows that Venmo, Facebook, Zoom, Snap, Slack, Tinder, Signal, Pinterest, Telegram, Chase Bank, Wayfair and even Samsung's smart washer will ask you for access to your Contacts. The list of apps seeking access to your Contacts is undoubtedly huge.

Sometimes, apps will restrict access. In iOS, third-party apps with permission can access any contact field, except for the Notes section, which requires additional approval from Apple. The company added that restriction in 2019, but it declines to say how many or which apps are cleared to access Notes.

Some will access just the basics – name, phone numbers and email address. Others will take anything they can get. Disabling the app's privileges doesn't necessarily result in the app

deleting information it already has. An app may – or may not- give you instructions on how to delete previously obtained information.

Apps Have a History of Misconduct

It has often been said that data is "black gold." So, if companies can get your data, they will. They will use it to advertise themselves, to sell their products, and for countless other purposes. They can also sell your data to others.

Several companies over the years have settled with the FTC over how they collected or used data without user consent.

All the way back in 2013, documents provided by Edward Snowden proved that the National Security Agency was collecting millions of contact lists, often from email and instant messaging accounts, to find hidden connections and relationships between targets.

Perhaps more significantly to lawyers, contacts have been leaked in data breaches. Once those Contacts are out there, there is no way to call them back. They almost certainly will be misused. Wire fraud and business email compromises are frequently the objectives.

Back to Ethics . . .

Like New York, most states have a rule that similar to this one:

Rule 1.6(c) of the New York Rules of Professional Conduct (the "Rules") requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to" the confidential information of current, former and prospective clients. Rule 1.6(a), in turn, provides that confidential information "consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

The opinion points out that the client is more likely to find that disclosure of the fact of a current or prior representation by a lawyer is embarrassing or detrimental where the representation involves or involved criminal law, bankruptcy, debt collection or family law. It strikes us that many high level executives, politicians, celebrities, etc. would consider their contact information highly confidential and would not be happy to have it (however inadvertently) disclosed by their lawyers.

Final Words

As we previously noted, our digital forensics work has exposed us to many contact lists of clients, including those of attorneys. Contacts are frequently used, especially in the Notes section, to record in brief very sensitive personal data that attorneys want to be able to reference quickly. But besides being alluring to advertisers and the like, such information, in the

hands of cybercriminals, can be used to compromise clients in a host of ways. We applaud the New York opinion which shines a bright light on the sensitivity of Contact data and the duty of lawyers to protect all data which may be confidential.

Our advice? Whenever an app wants you to consent to sharing Contact data, **JUST SAY NO!**

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker, and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity, and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.

Michael C. Maschke *is the CEO/Director of Cybersecurity of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744), a Certified Ethical Hacker, and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*