

LAW PRACTICE MANAGEMENT



What's Available for the Mobile Attorney

By Nina Lukina

An increasing number of attorneys are adopting a mobile work style. In and out of the office, they are working from home, traveling to meet clients, and, as always, going to court, devices in hand.

A range of technology is available to support seamless mobile work. The right hardware and software, and some time spent getting used to them, let lawyers take advantage of the ability to work anywhere as they would in the office.

Connectivity

You can bring your own internet with a mobile hotspot. Standalone devices that range in price from \$20 to \$100 can provide you with internet wherever you go, whether it's the train home from the office or a remote cabin in the wilderness.

You probably already have a mobile hotspot on you. Many smartphones give you the option of creating a network connection for other devices. This will consume data, so be careful of this feature if your plan is not unlimited. Another drawback is that you won't be able to rely on your phone when it doesn't get service, such as in that remote cabin. In such scenarios, it's best to bring along a separate device, such as Verizon's JetPack, or Samsung's Mobile HotSpot. If your

firm has an IT department, it might have hotspots available for loan.

Many firms are issuing attorneys laptops that can be docked (more on docking below) in the office and connected to the firm's network via virtual private network (VPN) when they are taken on the road. Together with Wi-Fi connectivity and VPN, you can work on your laptop as if you were at your desk at work. Additionally, if the firm's standard desktop deployment is on the laptop and Outlook is in cached mode, attorneys can work with documents and email even without internet access. When you do get internet access, the emails and documents will sync with the network in the office via the VPN.

Hardware

As mentioned above, a docking station at work, complete with two or more monitors, keyboards, and phone, is a highly mobile-friendly setup that many firms have adopted in the last few years. Attorneys can plug in their laptops when they arrive and enjoy the full benefit of having large monitors to work on (studies show that multiple screens can boost productivity), and take the laptops with them when they leave, continuing their work at their next destination.

Powerful, lightweight laptops and laptop-tablet hybrids have entered

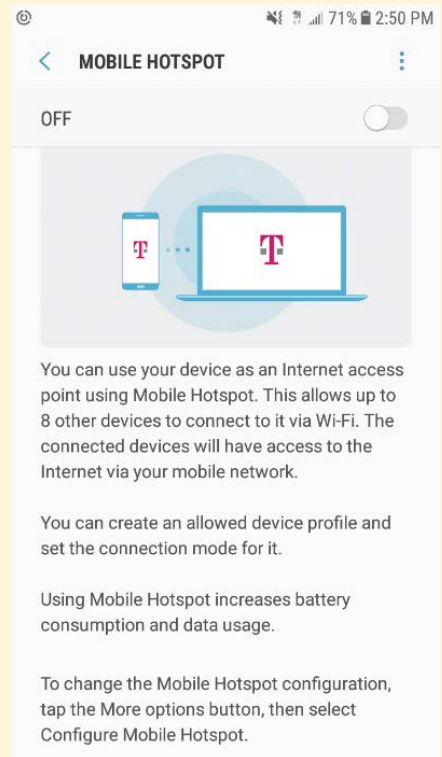


Figure 1 Mobile Hotspot Options on the Samsung Galaxy S7.

the market to meet the needs of this increasingly mobile workforce. The Surface Pro, an example of the latter, weighs two pounds, can be used either as a laptop or tablet, and features powerful processing and storage. Features such as handwriting-to-text translation make it a leading option among attorneys. The Lenovo ThinkPad Carbon is another popular lightweight Windows device.

Blank Rome LLP credits a 2015 firm-wide Surface Pro rollout with boosting efficiency, productivity, and associate happiness.

Laurence Liss, the firm's CTO, told *LegalTech News*, "We're trying to cut back on paper and make people more productive by being able to move around, and also more responsive to our clients and their colleagues. For

NINA LUKINA is a Marketing Associate in the New York office of Kraft Kennedy. She researches and writes about emerging topics in technology. A former consultant at Kraft Kennedy, she's worked on many IT strategy and information security projects for law firms.

example, people now can obviously take their tablets to meetings, to other peoples' offices, and they have all their documents or their emails at their fingertips."

Applications and Documents

With the tools described above, attorneys can empower themselves to work smoothly wherever they go. Some may want to take it further, however, and work not only on their laptops but

or tablets. Programs like Citrix, on the other hand, allow you to log in to your desktop from an iPad. Many attorneys are already relying on Citrix for snow days and other work-from-home occasions.

Staying Secure on the Go

Laptops are sadly prone to being left in taxi cabs and airport lounges. The trove of confidential client data on a typical work device makes security-

editions of Windows. Anyone working with privileged data should strongly consider this option.


As mentioned above, a VPN is highly recommended for working from places like coffee shops and hotels, which typically have insecure connections.

Most modern laptops and some phones also come with fingerprint readers, which simultaneously boost security and convenience. Mobile attorneys take advantage of them to sign in quickly and employ tight security. Mobile device management (MDM) solutions, such as Microsoft Intune, give you and your IT department control over mobile devices and laptops. If they are lost or stolen, for example, they can be remotely wiped. Finally, consider a privacy screen protector, which not only keeps curious and prying eyes from your client's emails but also reduces glare, allowing you to enjoy the sunshine while you work.

Many attorneys are already relying on Citrix for snow days and other work-from-home occasions.

on other devices. For that, many of the most common legal applications, such as the document management system NetDocuments and the billing programs like Rippe Kingston and 3E Elite, offer cloud implementations that can be used as apps on smartphones

conscious attorneys rightfully wary of the mobile work style. This is an uncomfortable scenario, but it can be made less stressful with measures such as BitLocker, a full-disk encryption feature that prevents unauthorized access. BitLocker is included with Enterprise



NYSBA CLE

Introduction to Discovery and Use of Electronic Information

Wednesday, March 14, 2018 | 2:00 p.m. – 5:00 p.m.
3.0 MCLE Credits in Skills

Program Chair
Ronald J. Hedges, Esq. | Dentons US LLP


Electronic information seems all-pervasive and, unsurprisingly, is a common feature of civil litigation. This program will introduce attorneys and support personnel to the NY and federal rules that govern discovery of admissibility of electronic information as well as the imposition of sanctions for its loss. The program will explore the "basics" of those topics and inform attendees on how to begin to think "electronic."

<p>1:30 p.m. – 2:00 p.m. Registration</p> <p>2:00 p.m. Introductions</p> <p>2:05 p.m. Part 1</p> <ul style="list-style-type: none"> • Overview of governing federal and state rules • The duty to preserve • Search and production • Protection of attorney-client privilege and work product 	<p>3:20 p.m. Break</p> <p>3:25 p.m. Part 2</p> <ul style="list-style-type: none"> • Discovery from non-parties • Discovery of social media • Sanctions • Admissibility <p>4:50 p.m. Q&A</p>	<p>5:00 p.m. Adjournment</p> <p>Program Faculty</p> <p>Gail Gottehrer, Esq. Akerman LLP Ronald J. Hedges, Esq. Dentons US LLP Shawndra G. Jones, Esq. Epstein Becker Green Hon. Shirley Werner Kornreich New York State Supreme Court, Commercial Division, New York County</p>
--	--	---

NYSBA Members: \$95 | Non-Members: \$195
Commercial and Federal Litigation Section Members: \$75
www.nysba.org/IntrotoDiscovery

www.nysba.org/cle Register online or call **1.800.582.2452**

The New York State Bar Association Has Been Certified by the New York State Continuing Legal Education Board as an Accredited Provider of Continuing Legal Education in the State of New York.





How *Not* to Use a “New” Technology to Share Privileged Information

By Ronald J. Hedges

As volumes and varieties of electronically stored information (ESI) increase, so do means to share and communicate ESI. When attorneys share or communicate ESI they must do so by means that maintain client confidences under New York Rule of Professional Conduct Rule 1.6(c) (RPC), which provides that attorneys “shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to,” confidential (“protected”) information. Failure to do so may have ethical consequences for attorneys. That failure may also result in waiver of attorney-client priv-

ilege, as demonstrated in *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*¹

The plaintiff insurer in *Harleysville* filed an action seeking a declaratory judgment that it did not owe the defendants (its insureds) for a fire loss claim. In the course of discovery an investigator for the insurer’s parent placed video surveillance footage on an “internet-based electronic file sharing service.” A hyperlink to the site was provided to the National Insurance Crime Bureau, which accessed the footage. Thereafter, the investigator placed the entire claims file onto the site to be accessed by the insurer’s attorneys. The site was not password protected

and the insurer conceded that anyone who used the hyperlink could access the site.

The insureds’ attorneys subpoenaed the Bureau, and the Bureau produced, among other things, an email from the insurer with the hyperlink. Defense counsel accessed the site, downloaded the claims file, and reviewed it without any notice to the insurer. The insurer learned of the access when, in response to a discovery request, the insurer produced a thumb drive that included confidential materials. Not surprisingly, the insurer moved to disqualify defense counsel.

RONALD J. HEDGES is a member of Dentons' Litigation and Dispute Resolution practice group. He has extensive experience in e-discovery and in the management of complex litigation and has served as a special master, arbitrator and mediator. He also consults on management and discovery of electronically stored information (ESI). He was a U.S. Magistrate Judge from 1986 to 2007 and is the principal author of the third edition of the Federal Judicial Center's *Pocket Guide for Judges on Discovery of Electronic Information*, available under "publications" at the FJC website.



sufficient to trigger an obligation on defense counsel to contact the insurer or secure a ruling from the court before reviewing the claims file and required them to bear the cost of the motion.

What might *Harleysville* teach? First, attorneys and their clients should be expected to use electronic means to share ESI. Those means might be unfamiliar to an attorney. Second, attorneys should familiarize themselves with any means selected to share ESI and determine what reasonable steps should be taken to avoid inadvertent disclosure and possible loss of attorney-client privilege or work product protection. Third, attorneys should counsel their clients to take reasonable steps.

These lessons are also apparent from Formal Opinion 477R of the American Bar Association Standing Committee on Ethics and Professional Responsibility (revised May 22, 2017), *Securing Communication of Protected Client Information*:

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

Electronic communication of information is common in the practice of law today. As *Harleysville* teaches, and Formal Opinion 477R points out, attor-

neys must make reasonable efforts to protect against any inadvertent disclosure that might lead to waiver of the attorney-client privilege and work product protection and also to ethical consequences. ■

1. No. 15cv00057 (W.D. Va. Feb. 9, 2017).

Applying the privilege law of Virginia, the court denied the motion. The court focused on several factors in doing so: (1) There was no evidence that the insurer had taken any precautions to prevent the disclosure in issue, let alone "reasonable" ones; and (2) the claims file remained accessible on the site for six months or more although the insurer "knew – or should have known – that the information was accessible on the internet."

As the court stated, "Harleysville has conceded that its actions were the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it." The court then applied the federal law of privilege and concluded that the insurer had also waived work product protection.

Several questions remained for the court: "whether defense counsel acted properly under the circumstances and whether any sanction should be imposed." The court found that a confidential notice contained in the email that transmitted the hyperlink was

CONNECT WITH NYSBA

Visit us on the Web:
www.nysba.org

Follow us on Twitter:
www.twitter.com/nysba

Like us on Facebook:
www.facebook.com/nysba

Join the NYSBA
LinkedIn group:
www.nysba.org/LinkedIn

