What the Patreaus Scandal Tells Us About Email Privacy

By Christopher B. Hopkins

Within a week of the release of the James Bond spy thriller, *Skyfall*, we learned that real-life superspies are not always as clever as their fictional counterparts. The details of General Patreaus' affair and resignation will likely come out in full detail. As of this writing, we have learned that the top spymaster of the CIA (Gen. Patreaus) used a public server email account (Gmail) to exchange emails with his mistress (Ms. Broadwell) who then misjudged the anonymity of using another email account to send "harassing" emails to a Tampa socialite (Ms. Kelley) who contacted the authorities. Investigating the Broadwell-Kelley emails, the FBI obtained IP address information from Google and tied Broadwell's once "anonymous" emails to the account shared with Patreaus.

Our clients, colleagues, and families use email on a daily basis and it is increasingly an obligation on every lawyer to understand the preservation of email evidence. The lesson: there is no delete. As we will discuss, remnants exist on your machine and there is an easily recoverable trail back across the internet – even if fake email accounts are made and emails are never actually sent.

From a historic standpoint, General Patreaus should have learned a lesson from his predecessor, former CIA director John Deutch, who indiscreetly kept classified information on an unclassified laptop (i.e., one that was connected to the internet). An investigation into Deutch's breach began in the CIA, was referred to the Department of Justice, and ultimately ended with a pardon by President Clinton during his final days in office. The lesson from the pre-Google era: do not put sensitive information on "unclass" computers which are *presumed* to be compromised.

Instead, General Patreaus opened a Gmail account which resides on the public servers at Google, the world's largest search engine. Would James Bond – or your teenager – store secrets there? We can likely assume that he did not read the Google privacy statement which confirms that Google "scans and processes all messages." Moreover, go into your own Gmail, Yahoo or Hotmail account – the margins are riddled with personalized ads, even in the draft folder – a sure sign that what you are typing is not For Your Eyes Only.

Google publishes a biannual Transparency Report which reveals that, since 2009, "government surveillance is on the rise." See Google.com/transparencyreport. Just in the last six months, Google handed over to the government information on 34,614 accounts – which is 5,769 accounts per day, every day.

Ironically, it was their weak clandestine efforts which lead to the discovery of the Patreaus-Broadwell affair. As we learned after September 2001, a common terrorist method of communication was to open a single account where party A would write an email, save it, and party B would log onto the same account, read the draft, and delete it. Thus, emails could be exchanged without the risk of being sent out over the internet. To further shroud this method of communication, the conspirators might open thirty phony email accounts and use one per day of the month, always moving, and sometimes accessing the accounts from library or internet café locations (those latter obfuscating steps were overlooked by Patreaus and Broadwell). Here, once the FBI began investigating Broadwell for her "anonymous" emails to Kelley, they quickly saw that she was accessing the account which connected her to General Patreaus. Hence the irony: if Broadwell had simply sent emails, as opposed to accessing a joint account, her communications should not have raise security concerns.

Everyone's downfall was the humble IP address, a 128-bit code which is akin to a license plate for each device connected to the information highway. An Internet Protocol address is a series of numbers and periods (like 123.45.678.9) which identifies every machine on the internet – among other things, it reveals your network and its location. For example, an email from me to you will have, buried in the header, an IP address next to "Received from." If you paste that IP address into websites such as IPTrackerOneline.com, IP2Location.com or Networksolutions.com/whois/index.jsp, you will quickly see that my email came from the domain Akerman.com in Florida. And those steps take mere moments – from there, a civil subpoena or warrant to the network provider will lead to the sender's computer. Here, the FBI obtained Broadwell's IP address from the "anonymous" emails she sent Kelley and then, armed with a warrant, the FBI was then investigated what other accounts her IP address was accessing (as noted above, Google is liberally handing over information about nearly 6,000 account *every day*).

Once an email is written, it is clear that public servers like Google are "scanning and processing" it. Like any cloud provider, they are presumably making a backup. Your computer, likewise, leaves some residue of your communications. Every time your computer accesses a webpage, it logs that step to speed up the process for future visits (into "cached DNS entries" as well as in a index.dat file). If the site you visited uses Flash, the notoriously hard-to-remove Flash cookies on your machine will further betray details of your path. If you need this information in your cases, consider a well-worded subpoena to ISP providers seeking IP address information; likewise, retain a forensic computer expert who can inspect the subject computer/device for remnant information.

Christopher B. Hopkins is a shareholder at Akerman Senterfitt. Bravely send your easily-identifiable email communications to Christoper.Hopkins@Akerman.com.

Circuit Court Report

CIVIL DIVISIONS • As of November, 2012

DIVISION	JURY TRIALS	NON-JURY TRIALS	MOTIONS	CASES PENDING
AA KELLEY	04-13	04-13	02-13	1356
AB KASTRENAKES	05-13	05-13	03-13	1374
AD FRENCH	03-13	03-13	02-13	1410
AE MCCARTHY	04-13	04-13	01-13	1572
AF KEYSER	06-13	06-13	01-13	1378
AG CROW	04-13	04-13	12-12	1499
AH BROWN	04-13	04-13	12-12	1304
AI SASSER	03-13	02-13	12-12	1064
AJ ROSENBERG	04-13	04-13	01-13	1177
AN McSORLEY	04-13	04-13	02-13	1508
AO BRUNSON	04-13	03-13	12-12	1510