New Jersey Law Journal

VOL. 210 - NO 12 DECEMBER 24, 2012 ESTABLISHED 1878

IN PRACTICE

FAMILY LAW

Protecting One's Privacy In the Digital Age

What kind of electronic trail are you leaving, and who can follow it?

By Steven J. Eisman

In the wake of the FBI investigation that ended the career of the director of the CIA and implicated the top American commander in Afghanistan, Americans have a renewed interest in protecting their digital privacy from the government, strangers and even their own spouses. As we continue to learn about the digital trail left by all parties in the military general scandal, individuals should be more aware of their digital rights and even consider legal channels to protect themselves. On the Internet, and especially in emails, text messages, social network postings and online photos, our work lives and personal lives are inextricably intertwined. Private, personal messages and keystrokes are stored for years on computer servers, available to be discovered by government investigators and snooping spouses alike.

The FBI investigation of General Petraeus began after socialite Jill Kelly complained to the FBI about receiving anonymous, harassing emails. The FBI commenced a cyber-stalking investigation, which revealed that Paula Broadwell, Petreaus' biographer and mistress, sent Kelly provocative emails threatening her to stay away from Petraeus. The FBI followed the electronic trail and gained access to Broadwell's Gmail account, whereupon they discovered her relationship with Petraeus through unsent messages in a drafts folder. The Stored Communications Act of 1986 requires only an administrative subpoena for government entities to ascertain the identity, bank account number, home address and other proprietary online information. Administrative subpoenas allow interested agencies to gain access to "private" digital data, such as email accounts and other online forums. Internet companies have reported an increasing amount of government requests. Google, for example, reported that it received more than 12,000 requests for user data from American government agencies in 2011, and that the majority of these requests were complied with. The U.S. Justice Department's manual on seizing electronic records states it can access emails that have been opened, those in the "sent" folder and all emails that are older than 180 days with a mere subpoena rather than a warrant obtained by a magistrate. And, of course, the government's reach is not restrained to email alone but rather includes legally obtaining a wide array of electronic information and communications, such as a user's location, keystrokes, transaction logs and all other "metadata" associated with online communication.

Many Americans are calling for an update to privacy laws in order to keep pace with the digital age. The Fourth Amendment protects against "unreasonable searches and seizures" in one's home and the U.S. Supreme Court has ruled that individuals have a "reasonable expectation of privacy" in phone conversations and in handwritten letters, however the same cannot be said for emails. The U.S. Supreme Court has not yet ruled on a case concerning email privacy. However, some jurisdictions are beginning to scrutinize the government's expansive access to electronic communications. In 2003, a federal court in California held that the government cannot legally have access to any emails more recent than 180 days old without a warrant. And, in 2010, a federal court in Ohio found that the Fourth Amendment protects email of any kind. Despite the movement toward protecting digital privacy from government interference in certain jurisdictions, the Stored Communications Act of 1986 and the Electronic Communications Privacy Act of 1986 continue to provide the government access to a broad range of electronic communications for the

Eisman is an executive partner at Abrams, Fensterman, Fensterman, Eisman, Formato, Ferrara and Einiger LLP in Lake Success, N.Y., and a fellow of the American Academy of Matrimonial Lawyers. Hilary F. Casper, a law clerk at the firm, assisted in the research and writing of this article.

majority of Americans.

Furthermore, in addition to the prying eyes of the government into our online activity, many would argue that we have just as much or perhaps more to fear from access to and disclosure of private digital information by significant others and spouses. In fact, the government is held to a higher standard when it comes to electronic interception of digital property. While the government has more power to electronically intercept and extract digital data, they still have to perform to the letter of the law. The "fruit of the poisonous tree" doctrine is an exclusionary rule which mandates that evidence obtained from an unreasonable search by a government agent must be excluded from trial. The same doctrine does not apply to searches done by non-government actors. If an individual's digital data is not properly protected, the average person may surreptitiously obtain such information — like emails or keystrokes — and that information may still be admissible in court.

Evidence like email, cell phone records, social networking records and even GPS and EZPass information is being used in divorce proceedings and custody disputes with increasing frequency. A study done by the American Academy of Matrimonial Lawyers (AAML) in 2010 found that an overwhelming 81 percent of the nation's top divorce attorneys say they have seen an increase in the number of cases using social networking and other online evidence during the past five years. And, a more recent report by the AAML in February 2012 found that 92 percent of lawyers surveyed had seen an increase in evidence from smartphones the past three years, citing in particular text messages, emails, call histories and GPS location information.

Parties to divorce litigation often request orders from the court allowing them to investigate a spouse's computer or obtain copies of cell phone records. In many cases, however, courts are asked to rule on the admissibility of electronic evidence which has already been retrieved. There are state laws prohibiting computer theft, trespass and invasion of privacy. But, in the context of domestic disputes, the lines are frequently blurred. If the electronic evidence was downloaded from a cell phone or a personal laptop of a spouse, many courts have ruled that this evidence is not admissible. Generally, if the devices are password protected, and therefore not ordinarily accessible to the person who has "broken into" them, or are not owned by the person who is seeking to use the data, such evidence is likely to be excluded at trial. On the other hand, if the electronic evidence is from a family computer, or from an email account in which the spouse shared the password, a social networking site, or text messages and emails exchanged between spouses, many courts will rule that such evidence is admissible. Divorce and privacy laws vary across state lines, and it is far from settled whether electronic evidence discovered by a "snooping" spouse is admissible in a divorce proceeding. Nevertheless, if the information is used to harass or intimidate someone, an individual can face prosecution for stalking or related offenses.

Reasonable expectation of privacy in marriage is complex. Courts across the nation are divided on this issue, and as such the legality of spying on a spouse can be quite complicated. Five of the 13 federal circuit courts have determined that surveillance is not allowed in a marriage, based on the Federal Wiretap Act. In a 2011 case, a Nebraska court held that a mother who concealed an audio recording device in her daughter's teddy bear for the purpose of gathering evidence to sabotage the custody rights of the girl's father was guilty of violating the Federal Wiretap Act. And, in 2008, an Iowa court ruled that a husband had unlawfully invaded his wife's privacy by taping her with a camera concealed in an alarm clock located in her bedroom in their home.

In New York, however, courts have ruled that interfamilial wiretapping in the midst of mere domestic conflicts is not a violation of the Federal Wiretap Act. Likewise, there is authority nationwide permitting wiretapping by one spouse of the other spouse and their child, for use in divorce and child custody hearings. In many cases the courts have used a vicarious consent argument, in that the one parent who wiretaps has consented on behalf of the child. The Federal Wiretap Act requires at least one party to the conversation to consent.

While the laws concerning e-discovery and electronic evidence are unsettled both within and across state and federal lines, there are several measures which may be taken to better protect your digital data and preserve the privacy of your online communications. In order to ensure that damaging digital evidence will not be a source of courtroom fodder or embarrassment, spouses should have separate computers, phone plans, iPads, etc., or at the very least, use secure passwords kept secret from their partner. In addition, bear in mind that any information posted on social media sites, such as Twitter and Facebook, may become public knowledge, even if the websites have "privacy" settings in place.

To confront the potential pitfalls of e-discovery and electronic data, a "digital privacy clause" can be included in a well crafted prenuptial agreement. Similar to an "infidelity clause," couples should consider inclusion of a digital privacy clause in a prenuptial agreement to protect themselves from any type of digital discovery by a spouse or partner in a divorce or custody dispute. Individuals concerned about their digital privacy and their right to protect their online communications should consult an experienced attorney who can address their particular circumstances, needs and goals. ■