OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXIV NUMBER V
MAY/JUNE 2017
www.mnbar.org

Bench&Bar OF MINNESOTA

GRAVE MATTERS

The law and practice of disinterment, reinterment, and exhumation in Minnesota

Why You May Need an LLC Update

Your Personal Data – Or Is It?

An Out of Court Article on Hearsay

RENEW YOUR MSBA DUES AT:
MNBAR.ORG/RENEW

Your Personal Data – Or Is It?

Doxxing and online information resellers pose threats to the legal community

By Mark Lanterman

Photo © iStockphoto

Given the sensitive nature of the courtroom and of the emotions that may arise there, attorneys, judges, and others in the legal community are at particular risk of becoming victims of doxxing-related crime. *Doxxing* is a term used to describe the buying, selling, gathering, posting, or distributing of private information online. Importantly, doxxing is typically carried out with malicious intent and is often aimed at damaging someone's reputation. As opposed to the mere gathering of information from someone's Facebook or LinkedIn profile, doxxing is often abetted by targeted data breaches. The distinction here is that anyone who posts on social media is essentially allowing the public at large to view, and use, that information. The kinds of private information spread through doxxing are not typically shared by the subjects themselves.

Everything from health to legal information is valuable to cybercriminals and hackers, and it is therefore exactly the kind of information that is commonly put on online. Apart from financial data, information related to health and legal circumstances can be of particular interest to an individual interested in harming another's reputation or career. Unfortunately, many doxxing victims don't realize that they have become victims until something serious has occurred or they realize that the information has already been widely distributed.

Though the personal information-gathering associated with doxxing can often be assisted by cyberattacks, doxxing itself is not necessarily illegal. Many people are not aware that their private information is widely available on personal information reseller websites. These websites are easily accessible by the average user, no Dark Web required. The information contained on these sites can divulge where you live, who your past employers were, and can even connect you to the last person living in your home or apartment. Fortunately, these websites give people the ability to opt out and remove their information. The problem is that the actual time it takes to remove the info, or the processes required to achieve this, can be confusing or cumbersome depending on the website.

Furthermore, some of the websites do not directly store your private information, but rather give users a list of other websites that do. For this reason, the individual is left to chase down their information on a number of websites instead of just one. And the fact is, even if someone takes the time to opt out of each one of these websites, it is very possible that they will repopulate their sites within a matter of months with the same information you requested be taken down. With this in mind, I would say that the majority of people are not aware of exactly how much private information is available about them online at any given time.

Private information can be used to physically stalk, harass, or threaten individuals. But it can also be used to harm a person's reputation or disrupt the victim's personal life. Recent headlines have focused on judges that have been targeted; however, everyone in the legal community is at an increasing risk of having their private information accessed without consent or knowledge. Given the rise of the Internet of Things (IoT), more and more data from our daily lives is being collected, stored, and distributed. Though this may be convenient, more data makes for a greater risk that it will be compromised. The number of devices comprising the IoT also makes for a wider array of potential access points for the cybercriminal. Since the process of doxxing often relies on the successful execution of data breaches, the Internet of Things presents the perfect blend of vulnerabilities and useful data.

The legal community is not immune to the changes brought about by the IoT. Living in a world of interconnected devices makes for easier communication, more efficient workflows, simpler data collection and storage, and a generally

OPT-OUT FORMS FOR MAJOR PERSONAL INFO RESELLERS

LINKS	VERIFICATION NEEDED	TURN-AROUND TIME
pipl.com/help/remove	Pipl is a search engine that does not host personal information, but it is a good starting point for identifying personal information from other sources.	Depends on other sources from which Pipl populates its search results.
www.beenverified.com/optout	Email address	24 hours in most cases
www.checkpeople.com/optout	None	7-14 days
www.intelius.com/optout.php	Government-issued ID	7-14 days
www.peoplesmart.com/optout-go	Email address	Up to 72 hours
www.publicrecords360.com/optout.html	State-issued ID	This site does not disclose turn-around time.
www.spokeo.com/opt_out/new	Email address	30 minutes
support.whitepages.com	Email address and phone number	Immediate
www.zabasearch.com/block_records	Redacted state-issued ID card or driver's license	4-6 weeks
www.zoominfo.com/lookupEmail	Email address	"Within a few days"
www.familytreenow.com/optout	Email address	Unknown

more productive way of managing things. Smartphones and Wi-Fi-connected devices mean greater accessibility and use of our personal information; for many IT departments, this convenience is the most important consideration when developing new technology policies. But the IoT is as risky as it is convenient. Many people don't understand the sheer amount of data that is being produced and stored about them. And each connected device is essentially another access point for a cybercriminal to compromise this data. For the same reasons that connectivity is great for communication, it is detrimental for security and keeping vulnerabilities contained.

In addition to providing opt-out information in this article, I will also provide some realistic risk-management advice. While it often feels as if the expansion of our digital lives is necessary, taking stock of the risks is important in managing security. For those in the legal community, developing a sound cybersecurity protocol is not only a responsibility to clients. It is also an important step in protecting your own privacy and keeping your personal information safe.

When assessing your current cybersecurity strategies, try to look from the outside in. Identify what data is most important and valuable. Also try to figure out where this data is currently being kept and what measures are in place to safeguard it against cyberattacks. Issues of employee compliance or outdated policies may arise during this examination, but making this kind of assessment is a very important step toward improvement.

To help those who are interested, I'm listing the names of several major personal information resellers and corresponding information about how to remove your personal data from their websites.

Opting out of personal information reseller websites is a solid step toward bettering your online behaviors. Keeping private information secure is not automatically guaranteed, especially when there are websites that profit from selling your info to anyone who might be interested. And like other cybersecurity protocols, checking these kinds of websites should be done fairly regularly. Opting out only removes the information that is currently posted; it doesn't necessarily prevent one of these websites from re-populating with your personal information in the future. Also, bear in mind that it is important to be proactive when it comes to removing your information the first time. Be mindful of the websites' turn-around times and don't let your opt-out request fall of your radar, or theirs, in the meantime. Though it may seem like an annoying chore, for those that are worried about becoming victims of doxxing, it is well worth the effort.

Like many changes that have arisen with the Internet of Things, doxxing is yet another issue that may affect you. Being mindful of what data you are sharing through your digital devices and doing your best to monitor your online presence are important elements of your personal cybersecurity strategy. Protecting your personal information is ultimately just as important as protecting your clients' data. ▲

***MARK LANTERMAN** is the chief technology officer of Computer Forensic Services. Before entering the private sector, Mark was a member of the U. S. Secret Service Electronic Crimes Taskforce. Mark has 28 years of security and forensic experience and has testified in over 2000 cases. He is an adjunct instructor for the University of Minnesota M.Sci. Security and Technology program, Mitchell Hamline Law School, and the National Judicial College in Reno, Nevada. Mark also conducts training for the Federal Judicial Center in Washington, D.C.*

✉ MLANTERMAN@COMPFORENSICS.COM