MIKE TONSING

Password Practices After *Szpyrka*

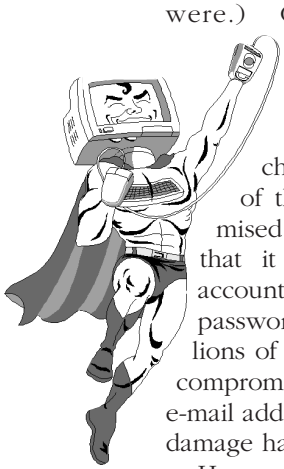
The subject of this month's column is your Cyberian passwords. At the risk of sharing news that will almost certainly be old by the time this column arrives in your in basket, I will begin by briefing you on a lawsuit that was filed on June 15, 2012, in the Northern District of California, where I live and work. (*See Szpyrka v. LinkedIn Corporation*, Docket Number CV 12-088HRL.)

Through the magic of the Internet, I have downloaded a copy of the class action complaint in *Szpyrka*. At the time this column was written, no responsive pleading had yet been filed so, for the most part, all I can give you is one side of the story. Ultimately, that won't matter—at least not in terms of the point that I want to make this month.

Szpyrka v. LinkedIn Corporation

On June 6, 2012, LinkedIn Corporation began looking into reports that a hacker had published a list containing 6.5 million of its users' passwords. Shortly thereafter, LinkedIn acknowledged that the theft had, indeed, occurred.

Affected users were notified by LinkedIn that it would be necessary for them to change their passwords immediately. (As of the time of this writing, there are very few clues as to whom the perpetrators were.) Other LinkedIn subscribers also were notified that their passwords may also have been compromise and they too were advised to change theirs.



LinkedIn apparently believes that what it characterized as quick action prevented any of the affected accounts from being compromised. And, LinkedIn's website quickly reported that it had received no reports of members' accounts being breached as a result of the stolen passwords. It also pointed out that, while millions of subscribers' LinkedIn passwords had been compromised, the passwords of their corresponding e-mail addresses had not. LinkedIn concluded that no damage had been caused to its subscribers.

However, within less than two weeks, Katie Szpyrka, a user of LinkedIn's services and a resident of Illinois, had filed a $5 million class action lawsuit with the Northern District of California in San Jose—adjacent to Silicon Valley, where LinkedIn's home office is located. While immediately acknowledging that "some security threats are unavoidable in a rapidly developing technological environment," Szpyrka alleged that LinkedIn's failure to comply with long-standing industry standard encryption protocols jeopardized its users personally identifiable information [referred to in the pleading as "PII"], and diminished the value of the services provided by Defendant—as guaranteed by its own contractual terms."

Szpyrka alleged that "LinkedIn's website states that it 'operates the world's largest professional network on the Internet with more than 120 million members in over 200 countries and territories [and] represents a valuable demographic for marketers with an affluent & influential membership.'" She pointed out that the privacy policy of LinkedIn set forth on its website vows that it will safeguard users' sensitive PII and states specifically: "all information that you provide will be protected with industry-standard protocols and technology." She claimed that LinkedIn had "deceived customers" by failing to meet its own announced high standard by having a security policy in place that was "in clear contradiction of accepted industry standards for database security."

Technology industry experts have already pointed out that in consumer security class actions it is very difficult to demonstrate actual harm, which is a legal requirement. Should it turn out that the hacker's breach of LinkedIn's security protocols was limited to customer passwords and did not involve the compromise of corresponding e-mail addresses, most industry analysts believe it will be difficult for the class action plaintiffs to prove that they were actually harmed by the hack. Thus, it is certainly possible that the *Szpyrka* lawsuit will not survive the inevitable initial legal challenges that will follow. On the other hand, Szpyrka's complaint specifically referenced a lawsuit filed against the "Guess?" clothing company wherein the FTC allegedly argued that, despite a posted policy insuring reasonable Internet security measures, Guess? actually "stored customers' PII in an unencrypted database concomitantly with poor website security"—alleging that the FTC had argued in *Guess?* that these practices constituted unfair or deceptive practices affecting commerce in violation of federal law. (*See in the Matter of Guess? Inc. and Guess.com Inc.*, available at www.ftc.gov/0S/2003/08/guesscomp.pdf.)

As you may or may not know, passwords used on an Internet site can be protected by a form of passwords security known as "hashes." Another form of passwords security typically used on top of hashing is called "salting." The *Szpyrka* lawsuit alleges that "industry standards require" at least the additional

process of "adding 'salt' to a password before running it through a hashing function." And, it further alleges that "this procedure drastically increases the difficulty of deciphering the resulting encrypted password." After the attack, LinkedIn closed the barn door, so to speak, by announcing that it was implementing a practice of salting passwords. And, a company spokeswoman was quoted in the *San Francisco Chronicle* as saying, "it appears that … lawyers are looking to take advantage of the situation." And, "we believe [Ms. Szpyrka's] claims are without merit, and we will defend [LinkedIn] vigorously against suits trying to leverage third-party criminal behavior."

We will see what comes of this. As I noted earlier, however, though the *Szpyrka* lawsuit is of more than passing interest, whether or not the plaintiff has a viable claim and whether or not she will pass muster as a suitable class action representative is not the point of this column.

The Point of This Column: Adopt Better Password Practices

Szpyrka v. LinkedIn—and lawsuits of a similar nature that have preceded it—should send off alarm bells for all Cyberian lawyers who use passwords (and who among us does not?). I have been as guilty as most of you in the way that I use passwords on the Internet. I have come up with two or three first-rate passwords and I have used them repeatedly in registering with different websites.

The password I use for online banking is the same as a password I use for online legal research and the password I use for my LinkedIn account is the same as the password I use for my personal Gmail account. The scary thing about the compromise of LinkedIn passwords is not that someone could get into my LinkedIn account and change the name of my former employer to Al Capone. Rather, it is that someone who knew my LinkedIn password could probably access many other websites that I use frequently by simply applying it there. That realization troubles me, and if you are doing the same thing I have been doing it should trouble you also.

If we weren't so foolish (and lazy?), we might have a very good class action lawsuit we could file. It is too difficult to commit 40 or 50 passwords to memory; it is much easier to remember two or three. But, especially for a lawyer who signs onto locations where confidential client information might be found, such foolishness and laziness cannot be easily excused.

What to do? Is the alternative really to commit 50 passwords to memory and to change them the first of each month?

Thankfully, the answer is no. Fortunately, for those of us who may admit to occasional foolishness and laziness, there is an altogether reasonable alternative. The solution to the titanic disaster foreshadowed by *Szpyrka* is to use a password manager.

Password Managers

As for password managers, there are currently five options. There are internal password managers that operate from inside your desktop computer. Portable devices like smartphones also can be used to store passwords. I do not recommend either of these options. Both of them have serious security flaws that should be obvious if you think about it for even a minute.

The third option is what is called a "token." A token is a combination of usually three things, often reducible to "something you have" (like an external memory card or a USB flash drive), "something you know" (an enabling PIN or password) and "something you are" (some sort of biometric recognition system—such as a finger scan or a face scan). Token systems are excellent but they present problems of their own, like the fact that "something you have" can easily be lost. And, they can be a bit cumbersome.

The fourth option is web-based password managers. Such programs store passwords on a provider's website. The fifth option is a so-called stateless manager, where passwords are generated on the fly from a master pass phrase and a tag using a key derivation function.

The best way for most of us to protect ourselves is option number four, a web-based password manager. Such a program can generate random passwords for all of your registered online accounts and then grant you access once you have proven that you are entitled to entrance. One such service is called LastPass™ (www.lastpass.com). LastPass can generate random strong passwords automatically and it can store them securely online, allowing you to access them from any internet-connected computer. LastPass is free for computers and $1 per month for smartphone users who have downloaded the LastPass app.

Once installed on your computer and given a strong password of its own, plus an e-mail address, the LastPass application will encrypt all of the logons and passwords stored on your computer. (Note: If you forget your master password you could be in serious trouble—especially if you've allowed LastPass to delete (as it urges you to let it do) all of the vulnerable logons and passwords on your computer.)

After that, to visit various websites that require a password, just log into LastPass and click the website you want to view. You will be logged on securely to the site you selected. LastPass also will complete the forms needed to buy goods and services online if you have stored your address, phone number and credit-card details, as well.

As a lawyer who travels, I had a lingering concern about LastPass: it's designed to store your passwords online. While I'm reasonably comfortable that they're safe from theft on their secure servers, what if the LastPass website goes down because of a hacker attack,

CYBERIA *continued on page 15*

The luncheon discussion was hosted by Duane Morris LLP.

Federal Litigation Section

On May 31, the Federal Litigation Section sponsored a dinner and reception for judges in the Eastern and Middle Districts of North Carolina. The event was held to allow local members of the bench to personally welcome their brothers and sisters who were visiting Durham, N.C., to study and teach in the inaugural class of the Center for Judicial Studies at Duke Law School. The program offers eight weeks of post-graduate legal education for active judges, leading to an LL.M. degree. Approximately 50 judges and other faculty attended the event with 30 members of the FBA and their guests. Among them were Hon. Sarah Parker, chief justice of the North Carolina Supreme Court. Dean David Levy of Duke Law School, who is a former federal judge of the Eastern District of California, introduced the speaker, Pulitzer-winning author Linda Greenhouse of Yale Law School. The section's vice-chair, Rob Kohn, convened the formal part of the evening by thanking the FBA's Chapter Activity Fund, which contributed support for the event, as well as leaders of the Eastern District of North Carolina and the Middle District of North Carolina Chapters. Camden Webb, president of the Eastern District of North Carolina Chapter, stated, "The event was a great occasion for our members to meet local North Carolina judges as well as judges from across the country who were attending the program. We also took the opportunity with this event to promote the benefits of joining the FBA and add members. I was grateful that we were able to participate in such a terrific event."

Section on Taxation

On June 26, the Section on Taxation held a program entitled "Women in Tax Law: Strategies and Perspectives on Tax Litigation," which was hosted by Mayer Brown LLP. The event featured a panel discussion which focused on strategies for developing a successful career as a tax litigator. Speakers included Hon. Christine O.C. Miller, U.S. Court of Federal Claims; Judith A. Hagley, senior litigation counsel, DOJ, Tax Division, Appellate Section; Elizabeth Girafalco Chirich, branch chief, IRS Chief Counsel; and Miriam Fisher, partner, Latham & Watkins LLP.

Younger Lawyers Division

The Younger Lawyers Division has continued sponsoring the Summer Law Clerk Program, which features various roundtables and site visits for law clerks, law students, and interns. On June 18, the Capitol Hill roundtable featured discussions from attorneys who are currently working in various offices on the Hill. The attorneys discussed their career paths and offered advice to students interested in working in or with the federal government on the Hill.

On June 22, the Department of Defense roundtable contained military panelists who discussed the duties, responsibilities, and unique life experiences of today's military attorney. Panelists included judge advocates from the U.S. Army, Air Force, Coast Guard, Marines, and Navy. The panel was co-sponsored by the Pentagon Chapter of the FBA.

On June 28, the Department of Justice roundtable featured speakers from various divisions of the department, including attorneys from the Civil Division, National Security Division, Tax Division, and the Criminal Division of the U.S. Attorney's Office of the District of Columbia. **TFL**

Sections and Divisions is compiled by Sherwin Valerio, FBA manager of sections and divisions. Send your information to svalerio@fedbar.org. Visit www.fedbar.org for the latest section and division news and events.

CYBERIA *continued from page 13*

or worse, because the company goes out of business? Would I forfeit the keys to my online life? The answer is no, because LastPass also stores the passwords on my computer where they're accessible through the browser. They cannot be changed or updated if the LastPass servers are down, but at least they're there.

An alternative brand to LastPass is Roboform.™ (www.roboform.com.) If you're shopping around, you should check it out. An additional option worth investigating is OpenID™, which can be investigated at en.wikipedia.org/wiki/OpenID.

None of these three choices is a complete answer to online security, of course. Even a smart lawyer like you could still be duped into entering a password on a fake "phishing" site set up to look like your bank's. And, were someone to discover your LastPass master password in your sock drawer or your purse, that person could get all your passwords at once from your online vault. In that sense, online storage of the passwords is riskier than having them on your computer.

But even if there are risks to using LastPass, OpenID, or Roboform, they are better alternatives than using the same password for all your sites. They are probably also safer than writing down all of your passwords on sticky notes and carrying them around with you, as I have sometimes observed other lawyers doing.

Conclusion

See you next month in Cyberia. In the meantime, please forward your universal password and username to my email address below, for safekeeping. **TFL**

Michael J. Tonsing practices law in San Francisco. He is a member of the FBA editorial board and has served on the Executive Committee of the Law Practice Management and Technology Section of the State Bar of California. See www.TonsingLawfirm.com. He also mentors less-experienced litigators by serving as a "second chair" to their trials (www.YourSecondChair.com). He can be reached at Mike@TonsingLawfirm.com.