Friday, January 23, 2015

Open-sourcing and crowdsourcing cybersecurity

By Hsiao C. (Mark) Mao and Victor Chen

AfterÂ *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), it appeared that defendants in cyberbreach cases could easily defeat most plaintiffs by arguing that plaintiffs have failed to show Article III standing. Cases following *Clapper* in 2014 taught us that although standing and damages are still difficult to prove, defendants may need to be prepared to fight on additional grounds.

As plaintiffs in cyberbreach cases still need to rely on theories of negligence, whether an organization took "reasonable" precautions remain critical. Industry trends and the recent mandates of the Obama administration suggest that organizations will increasingly look toward "open sourcing" and "crowdsourcing" for cybersecurity solutions.

New Battlegrounds: Moving On From Standing?

Although at issue in *Clapper* was the federal government's right to intercept communications pursuant to an amendment to the Foreign Intelligence Surveillance Act, the case had enormous implications for cyber-litigation. Many reading only the majority's opinion denying Article III standing believe that the respondents failed to present "damages," but that is not entirely correct. As the four dissenting justices stressed, one of the respondents claimed he had thousands of communications intercepted by the government, albeit prior to the passing of the amendment.

Defendants have since used *Clapper* with relative success, arguing the "mere" loss of data is insufficient to confer Article III standing. For example, in *In re Science Applications International Corp. Backup Tape Data Theft Litig*., MDL No. 2360 (D.C. May 19, 2014), backup tapes containing medical information of millions of individuals were stolen from the car of an employee. The class members alleged that they suffered increased risk of identity theft, and for at least one plaintiff, actual identity theft.

The trial court granted a motion to dismiss based on lack of standing, and the appellate court affirmed. Citing *Clapper*, the court rejected the plaintiffs' argument that they were more likely to suffer identity theft, noting the "degree by which the risk of harm has increased is irrelevant - instead, the question is whether the harm is certainly pending." Even had data been compromised, the court pointed out what the thieves intended to do or could do was entirely speculative, which is insufficient to confer standing.

The majority of subsequent cases continued to apply the *Clapper*-logic stringently, particularly where the plaintiffs have not alleged the actualÂ misuse of data. SeeÂ *Strautins v. Trustwave Holdings Inc*., 12-09115 (N.D. Ill. Mar.Â 12, 2014);Â *Galaria v. Nationwide Mut. Ins. Co*., 998 F. Supp. 2d 646 (S.D. Ohio 2014);Â *Polanco v. Omnicell Inc.*, 13-1417 (NLH/KMW) (D.N.J. Dec.Â 26, 2013);Â *In re Barnes & Noble Pin Pad Litig*., 12-c8617 (N.D. Ill. Sept.Â 3, 2013).

However, there is now doubt about whether *Clapper* will continue to be applied stringently. First, in *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL No. 11MD2258 AJB (MDD) (S.D. Cal. Jan.Â 21, 2014), the district court surprised many by permitting some of the claims to survive a motion to dismiss, although the plaintiffs did not allege that they suffered unauthorized charges.

Then in *In re Adobe Systems Inc. Privacy Litig*., 13-05226 (N.D. Cal. Sept. 4, 2014), the court permitted claims to survive a motion to dismiss, finding persuasive that hackers "deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, mailing addresses, and credit card numbers and expiration dates."

And in *In re Target Corp. Customer Data Security Breach Litig*., MDL No. 14-2522 (D. Minn. Dec. 18, 2014), the court found persuasive plaintiffs' alleged "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees," to defeat a motion to dismiss.

Perhaps a more cynical view is that Article III standing trends have not changed; instead, plaintiffs have become bolder in what they are willing to allege. Particularly in *Adobe*, plaintiffs pled that hackers targeted Adobe's systems with the specific purpose of obtaining payment information. It is unclear how plaintiffs intend to prove the specific intent of hackers they will probably never catch.

Nonetheless, these cases have also led experts to wonder whether California will now be the ground for plaintiffs' firms to focus their efforts, particularly as California continues to pioneer legislation and policies on data privacy. But seeÂ *Sutter Health v. Superior Court* (Atkins) (dismissing claims pursuant to California Medical Information Act for a stolen computer containing 4.2 million unencrypted patient records, because plaintiffs did not plead that confidential information was actually viewed).

In addition, these cases suggest that organizations should be prepared to defend cyber-litigation on more than just Article III standing grounds.

Using Open-Sourcing to Prove the Standard of Care?

On Jan. 13, the Obama administration and Department of Defense announced more zealous efforts to push for "information sharing among private-sector companies through private-sector-led information sharing and analysis organizations."

Preceding even the recent efforts of the Obama administration, those in the private sector have already been quietly organizing themselves. Many smaller and middle-market companies have found prevalent enterprise cybersecurity solutions too costly. Instead, they have tried to find greater security in the collective, leveraging lessons from software "open-sourcing" and "crowdsourcing" technologies. Companies exploring open-source cybersecurity solutions will find that there is a growing network of organizations implementing and improving open-source software solutions.

Open-source software has been relatively successful by promising participants a "free" license in exchange for their contribution in software development, and promise to offer similar licenses for their derivative products. Many experts argue open-sourced software is more "bug free" than traditional fee-based software, as the programming code is open to community assessment and development.

If cyberbreach cases move more easily past standing issues, defendants may have to explain how they took "reasonable" precautions. That their security solutions were openly tested and retested by a large community of similar users may be one way of proving reasonableness. One might argue that if tens of thousands of open testers could not find a new bug, why would it be unreasonable for a defendant to not have anticipated the new vulnerability?

Indeed, many bugs and loopholes with open-sourced software were first reported by licensees and developers, and the hope is that by open-sourcing cybersecurity solutions, users would have a vested interest in quickly reporting problems as they implement, test and retest the software. Hopefully, when the "crowd" is sufficiently large, developers looking for solutions to a bug would put other users on notice, before hackers can fully exploit the same bug.

The Obama administration's proposal is not the first time the administration has suggested more cooperation with the private sector. It remains to be seen whether Congress will agree with the administration, having rejected other cyber-legislation proposals from the administration previously.

Perhaps more importantly, it is not clear that the private sector would necessarily welcome information sharing with the authorities. After reports surfaced in 2013 about technology companies quietly complying with subpoenas from authorities such as the National Security Agency, companies like Apple, Facebook, Google and Microsoft began leaning towards notifying users of government seizure of data. Investigators and

authorities on the other hand, warn that such notification makes protecting against terrorist and criminal acts much more difficult. Although it is still unclear if North Korea is really behind the attack on Sony Pictures, it appears that the NSA is convinced that the attack is an example of why greater cooperation from the private industry is critical in preventing future cyberattacks.

Regardless of who is right, everyone seems to agree that success is more likely in the collective, and organizations trying to protect themselves from hackers should at least be as organized as the ones attacking them. Regardless of whether one believes in "open-sourcing" or "crowdsourcing," with or without help from the authorities, the success of organized hackers prove that those in the private industry needs to better communicate with each other on the nature of cyberattacks and vulnerabilities.

Hsiao C. (Mark) Mao *is a partner and vice chair of the Technologies Practice Group in the San Francisco office of Kaufman Dolowich & Voluck. You can reach him at mmao@kdvlaw.com.*

Victor Chen *is the director of legal affairs at AlienVault, Inc., a company that provides open-source data-security software solutions and services. You can reach him at vchen@alienvault.com.*