New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 124
TUESDAY, DECEMBER 30, 2014

CYBER SECURITY

The Sony Hack: Why Companies Must Review Network Security

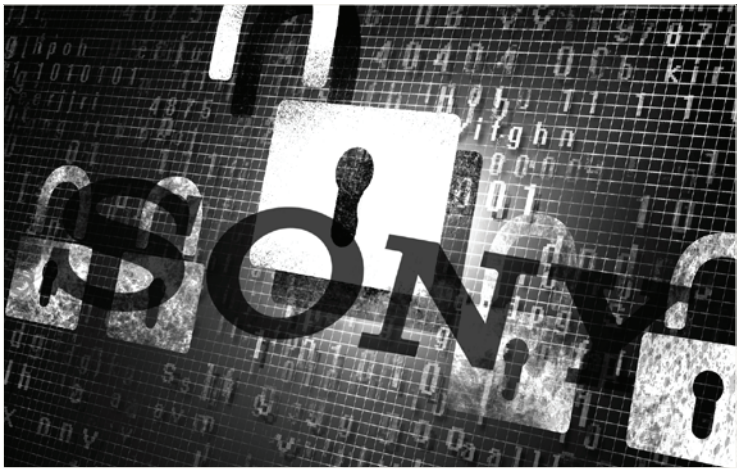
By **Karen H. Bromberg**

And **Duane A. Cranston**

In a year of major hacks, including cyberattacks on JPMorgan Chase, Home Depot, and Staples, the hack attack on Sony Pictures Entertainment may be singularly responsible for accelerating the public debate on cybersecurity in much the same way that Edward Snowden's revelations about secret government operations brought to the forefront the debate on digital privacy. The Sony breach is a wake-up call, not only because the hack was carried out with the principal aim of harming Sony, but because the ongoing leaks are likely to raise unprecedented legal issues for the company.

The Sony breach could be the lever that spurs action on the federal level to update security requirements for all companies that electronically store and transmit confidential personal information.

Over the course of the past several weeks, the widely publicized cyberattack on Sony has resulted in the public disclosure of confidential information of its employees and others, including names, addresses, email communications, over 47,000 Social Security numbers (including for Sylvester Stallone and Judd Apatow), health care data and other private information. U.S. agencies including the F.B.I. have stated that the security breach was either carried out, supported and/or sponsored by the North Korean government in retaliation for the planned release of "The Interview," a film that is critical of the government of North Korea. The breach has also led to the public posting of email communications among senior executives of Sony Pictures, which have been reported widely in the news media and have created a public relations nightmare for Sony.



BIGSTOCK

In the midst of these developments, four class action lawsuits have been filed by and on behalf of current and former Sony employees asserting that their personal information has been accessed and made public as a direct result of this security breach. Most of these lawsuits allege that Sony breached a duty of care in its administration of its security measures, including its response to this security breach once it had occurred, and also violations of certain state laws concerning the retention of medical information and the provision of notice to potential victims of the breach. Certain of these suits also allege actions under state laws concerning personal privacy and unfair competition.

Sony's Potential Liability

The breach of Sony's security differs from other recent breaches because this is the one instance in which U.S. government agencies have affirmatively attributed the breach to actions sponsored by a foreign government. This raises the issue of whether, and to what extent, a private company can foreseeably anticipate a network security threat from a state-sponsored actor and what resources a company could reasonably bring to bear to protect its systems from such an attack. And while this may be a unique scenario, past media reports have generally alluded to the existence of state-sponsored cyber-espionage for purposes of misappropriating trade secrets and other intellectual property, or to gain and exploit a competitive business advantage.

The class action lawsuits allege violations of California state laws including the California Confidentiality of Medical Information Act (Cal. Civ. Code §56, et seq.), the California Customer Records Act (Cal. Civ. Code §1798.80, et seq.), and common law negligence. The suits allege that Sony knew that its network had substantial vulnerabilities well in advance of the breach, particularly in light of a 2011 breach of its security network through its Sony PlayStation platform, and should have anticipated the potential for further damage that would expose confidential employee information. The majority of these suits also allege that Sony failed to respond to the breaches in accordance with the requirements of the breach notification provisions of §1798.80. These suits make various claims regarding the resulting harm from the breach, including harms stemming from the release of confidential medical information and invasion of privacy in violation of the California

KAREN H. BROMBERG *is a partner at Cohen & Gresser and head of the firm's intellectual property and technology group.* DUANE A. CRANSTON *is an associate at the firm.*

state constitution (Cal. Const. Art. 1, Sec. 1).

Each of these suits has been brought in a jurisdiction where privacy concerns have often been a primary focus of legislative and administrative action by the state. California is frequently at the forefront in enacting legislation to protect its citizens' privacy, introducing the first breach notification law in 2002, which went into effect in 2003. Today, 47 states and other U.S. territories have enacted their own breach notification laws, including Virginia, whose own breach notification statute (§18.2-186.6 of the Code of Virginia) was cited as a cause of action in one of the lawsuits. Following a 2012 report issued by the California Attorney General detailing security breaches in California, the state broadened the application of its breach notification law to require notification where any breach disclosed unencrypted names and email addresses in combination with passwords or security questions. One potential near-term consequence of the Sony data breach may be an additional collective response by other states to follow suit by broadening the protections of their data breach notification laws in similar fashion.

But Sony may be vulnerable to litigation in a way that other companies that preceded it have not. Plaintiffs traditionally have struggled with maintaining a cause of action for data breaches because of the difficulty they have in demonstrating that they suffered any actual injury. Here, however, Sony could be deemed in breach of the numerous non-disclosure agreements it likely has in place, whether with studios, talent, or otherwise. Parties to an NDA are generally subject to an obligation to maintain reasonable security measures to safeguard each other's personal and confidential information, and most often these agreements contain a provision that harm will be presumed in the event of a breach. Such a clause could arguably eliminate the Article III standing obstacle. The public disclosure of confidential information and transactions may render Sony in breach of its NDA provisions if it is found to have not taken appropriate precautions to avoid the hack. In the context of its prior PlayStation breach, and its possible failure to take remedial steps to guard against another, multiple claims could ensue.

Another area of concern is the high profile and celebrity status of many of the individuals whose confidential information have been leaked. There exists the strong possibility that claims for damage to reputation may ensue stemming from Sony's failure to take reasonable precautions to protect against the disclosure of such confidential information.

Federal Laws

While the four class action lawsuits concern personal information of Sony employees, the security breach has also resulted in the dissemination of confidential communications between Sony personnel and third parties. These disclosures have been publicized largely to the extent that they include comments and discussions regarding celebrities and other public figures. In this respect, the Sony breach resembles the Apple iCloud network attack, which similarly resulted in the release of confidential communications and was covered widely in the media.

One of the limited avenues of recourse available to celebrities whose personal content was redistributed across numerous websites following the iCloud breach has been the "take down" safe harbor provision of the Digital Millennium Copyright Act (the DMCA). Title II of the DMCA amends the Copyright Act by adding a section limiting the liability of Internet service providers (ISPs) for copyright infringement arising from certain uses of their services. The "take down" safe harbor protects an ISP from liability for infringing material that has been uploaded by third-party users to their systems, provided that the ISP did not have knowledge of the infringement, has not directly benefited financially from the infringement, and takes down the infringing material from its service upon receipt of notice of the infringement. In the case of the iCloud breach, victims of that security breach availed themselves of this "take down" provision to notify ISPs that the personal images and other material being published and redistributed through their services infringe their copyright ownership in these materials. Many, if not most, of the websites and other ISPs receiving such notices have complied with these take down requests.

The breach of Sony's security differs from other recent breaches because this is the one instance in which U.S. government agencies have affirmatively attributed the breach to actions sponsored by a foreign government.

These "take down" notices, and the compliant response of the media to them, are also in marked contrast to the Sony situation, where Sony's demand that stolen information not be published by media organizations has received a mixed reaction. Sony issued its demand through legal counsel. Certain news organizations have agreed to restrict their use of such material, where others have more broadly asserted that the material is news worthy and thereby constitutes "fair use." However, while this course of action may be used to limit the publication and redistribution of these images, it does not afford these individuals any direct recourse against the perpetrators of the breach, nor does it provide them with any right of action against Sony in connection with the security breach. Other federal legislation provides some additional protection for data security breaches. The Electronics Communications Privacy Act (the ECPA) imposes a privacy obligation on telecommunications providers, providing that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication … to any person or entity other than an addressee or intended recipient of such communication." The provisions of the ECPA referred to as the "Stored Communications Act" include a private right of action for individuals and companies whose information has been unlawfully accessed, setting out penalties for violators that include fines and even imprisonment. Unlawful access to digital information is additionally prohibited under the Computer Fraud and Abuse Act (the CFAA), which provides an additional private right of action for information security breaches.

The ECPA and CFAA were enacted in 1986, and many technology developers and service providers have challenged their application to services that have emerged in the nearly two decades since their enactment. Courts have also been somewhat split on determining what constitutes unauthorized access, with certain courts taking an increasingly limited view of the CFAA particularly with respect to alleged unauthorized access to companies' confidential information by former employees of such companies. Accordingly, lawmakers and industry groups alike have made policy recommendations and proposed new legislation to update the substantive provisions of the ECPA and CFAA and establish a more effective framework for the application and enforcement of their respective provisions, though none have yet been passed.

Conclusion

The confluence of notable security breaches over the course of the past several years seems to have reached a new degree of prominence in the public eye with the Sony breach, and particularly with respect to the debate around privacy and security. The Sony breach could be the lever that spurs action on the federal level to update security requirements for all companies that electronically store and transmit confidential personal information. While the focus on information security has largely been on the processing of financial and medical information, the framework could soon encompass any information that a company may store regarding its employees. At a minimum, in the wake of the Sony breach, the message to all U.S. businesses is clear: They need to take a hard look at their network security, invest in rigorous security systems, identify vulnerabilities on their networks and create a plan to work quickly to address them.