Amber Heard's Privacy

This column contains subject matter and references that some readers may find objectionable. ISACA® believes that the context of the subject matter makes it appropriate and necessary for the privacy discussion herein.

Evidently, Amber Heard is an actress in Hollywood. I say "evidently" because I have never seen any of her films or television shows. I first became aware of Ms. Heard when she published an article in *The New York Times* concerning nonconsensual pornography, often termed "revenge porn."[1] It seems that

> *…[in] 2014, hundreds of private, intimate photos of celebrities—most of them women—were posted on the online message board 4chan. From there, they spread to other online sites like Reddit, where the thread including links to the photos gained 75,000 subscribers in less than a day.*[2]

Pictures of Ms. Heard were among them. She was embarrassed, harassed and tormented especially because, despite all her efforts, the pictures keep reappearing on the Internet.

Privacy Laws

There are laws in most of the United States concerning revenge porn.[3] They are based on the premise that the person or persons who publish these images are harassing the victims. The law in the State of California, where Ms. Heard lives, without stating that the publication of nudity is not an offense, does explicitly say that the intent of the publisher makes it one.[4]

However, Ms. Heard makes the case that nonconsensual pornography is more than harassment; it is a violation of privacy.[5] There is some support for her position in the statute, which states, in part, that "the parties agree or understand that the image shall remain private."[6] But does the commonly used word "private" imply privacy as legally defined? It is at this point that Ms. Heard's argument becomes relevant for this esteemed *Journal*.

Federal privacy laws in the United States deal primarily with financial[7] and health-related information.[8] There are also privacy laws in every US state, but none, to my knowledge, address the publication of nude images without the consent of the subject. (In California, there is an exception to this statement, which we will return to later). So, in a legalistic sense, Ms. Heard's privacy claim regarding her pictures does not seem sustainable.

Amber Heard

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (*www.isaca.org/journal*), find the article and click on the Comments link to share your thoughts.

https://bit.ly/2UmOGC2

Steven J. Ross, CISA, AFBCI, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

In those countries subject to the EU General Data Protection Regulation (GDPR)[9] (or other laws based on it[10]), Ms. Heard has a better legal case, not so much because of the nudity, but because publication of *any* images without consent is prohibited.[11] There is no need to establish the right to privacy over nonconsensual pornography when all information, including images, is already established.

Malicious Intent

Thus, Ms. Heard (and anyone else so victimized) is faced with a conundrum. As she points out in her article, in the United States, publication of nonconsensual pornography is illegal only if bad intent (i.e., harassment) can be proven. She points out that "a personal vendetta wasn't what motivated the people behind the hacking of [her] photos."[12] The same act, though, is *de jure* illegal in Europe. For those who are involved in legitimate international commerce—and who would never publish pornography—the fact that the same act can be legal in one jurisdiction but not in another is indicative of the problems of establishing privacy over a global Internet.

Chief among these, from Ms. Heard's perspective, is not only that the pictures were published, but that they continue to be published. Many of the pornographers abide in Freedonia,[13] well beyond the reach of privacy or any other laws. This is why those pictures remain on the Internet.

The Right to Be Forgotten

What she is looking for is the right to be forgotten, as expressed in GDPR.[14] Importantly, in this case, the same concept is embedded in the US State of California Consumer Privacy Act (CCPA), which went into effect on 1 January 2020.[15] Specifically, the California statute says, "A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer." But is this section applicable? Is Ms. Heard a consumer? Were the pictures collected from her?

Further questions arise. What if the pictures were not of her in the nude but of her carrying a sign supporting a notorious political group? Or of her committing a crime? Does she have the right to privacy, for these pictures to be forgotten? And forgotten where? If she were convicted of a crime, information regarding that might be deleted from a search engine, but would still be retained in court records, available to the public.

In short, the requirements for achieving true privacy in information systems are not inherently obvious. We use the word "privacy" and its variants in many familiar ways: a private conversation; in the privacy of one's own home; my private hopes and fears. Are we implying privacy in the legal sense when we use these terms? Or, put the other way, do (or should) our privacy laws encompass all meanings of the word? For surely, as Ms. Heard writes, she had an expectation of privacy about those pictures.

> "SIMPLY DEFINING PRIVACY AS COMPLIANCE WITH THE RELEVANT LAWS MAY BE INSUFFICIENT AND CAN LEAD TO DEBILITATING LEGAL ACTIONS."

Policies and Standards

In the absence of clarity, I suggest that it is up to each organization to define its own intentions regarding privacy. As I have been saying here, simply defining privacy as compliance with the relevant laws may be insufficient and can lead to debilitating legal actions. The organization's privacy position should be enshrined in policy and standards.

It will be up to information security professionals to enforce those policies. Therefore, I recommend that those professionals be involved in devising and promulgating them. The professionals will have to build controls into systems to give the policies and standards force. Without being a party to their creation, information security people may find themselves in uncharted and ambiguous situations. Best to have a say at the outset.

Some years ago, I wrote a piece in this space entitled "Paris Hilton's Privacy."[16] In it, I concluded "[if] any of us are to have privacy, Paris Hilton must have it too." The same applies to Amber Heard.

Endnotes

1 Heard, A.; "Amber Heard: Are We All Celebrities Now?" *The New York Times*, 4 November 2019, *https://www.nytimes.com/2019/11/04/opinion/amber-heard-revenge-porn.html*
2 *Ibid*.
3 Cyber Civil Rights Initiative, "46 States + DC + One Territory Now Have Revenge Porn Laws," *https://www.cybercivilrights.org/revenge-porn-laws/*. The Cyber Civil Rights Initiative, founded by a nonconsensual pornography victim, is an excellent source of information on this topic.
4 California Legislative Information, California Penal Code Section 647(j)(4) PC Invasion of Privacy, *https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=647.&lawCode=PEN*. The specific statement is "with the *intent* to cause serious emotional distress" (emphasis added).
5 *Op cit* Heard
6 *Op cit* California Penal Code Section 647(j)(4)
7 United States Congress, Gramm-Leach-Bliley Act or the Financial Services Modernization Act of 1999, 12 November 1999, *https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf* (generally known as GLBA for the initials of its authors)
8 Centers for Disease Control and Prevention, Health Insurance Portability and Accountability Act of 1996 (HIPAA), USA, 1996, *https://www.cdc.gov/phlp/publications/topic/hipaa.html*
9 Intersoft Consulting, General Data Protection Regulation GDPR, Belgium, 2018, *https://gdpr-info.eu/*
10 Comforte Insights, "Six Countries With GDPR-Like Data Privacy Laws," *https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws.* That is, Australia, Brazil, Japan, South Korea and Thailand—California is also mentioned, but it is not a country (yet) and the comparison is inexact.
11 Intersoft Consulting, Art. 4 GDPR, Definitions, Belgium, 2018, *https://gdpr-inf.o.eu/art-4-gdpr/*. Specifically, "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."
12 *Op cit* Heard
13 Freedonia is my all-purpose, though fictitious, name for small, out-of-the-way countries beyond the reach of international law. It is taken from the Marx Brothers film *Duck Soup*.
14 Intersoft Consulting, Art. 17 GDPR, Right to Erasure ("Right to be Forgotten"), Belgium, 2018, *https://gdpr-info.eu/art-17-gdpr/*
15 California Legislative Information, California Consumer Privacy Act of 2018, Code Section 1798.105 (a), 2019, *https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.105.*
16 Ross, S.; "Paris Hilton's Privacy," *Information Systems Control Journal*, vol. 3, 2005. Paris Hilton was, at the time, a celebrity with less claim to the role than Ms. Heard.

Enjoying this article?

- Read *Enforcing Data Privacy in the Digital World. www.isaca.org/enforcing-data-privacy*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*