Venkata Aditya Bollapragada

Johns Hopkin University

vbollap1@jhu.edu

Attorney for Plaintiff

Heart2Heart

Plaintiff,

vs.

John Smith,

Defendant.

INTRODUCTION

The case brought in front of the court involves the Plaintiff Heart2Heart suing the Defendant John Smith. A pacemaker functions by detecting the heart rate of the patient the device is attached to, and generating a small electrical pulse in order to maintain a regular heartbeat in the patient. Normally, when it is initially installed, the pacemaker is connected to a hospital network, so the device can be monitored to ensure it is functioning properly. A company called *Heart2Heart* produces pacemakers for patients who recently suffered a heart attack and have irregular heartbeats The Defendant was a former employee of Heart2Heart. He was involved in the development of a pacemaker that Heart2Heart used to sell. After discovering a technical vulnerability that the Plaintiff chose not to address, the Defendant decided to quit the company due to moral issues. The vulnerability allows for exploits to be designed to gain complete access of the device and exposes sensitive parts of code hidden from general users. The nature of the vulnerability also only allows it to be discovered using tools and technology that are available and proprietary to the Plaintiff. Also, the only way to fix the vulnerability was by recalling all the devices that were already in circulation. Plaintiff decided to not go in that direction for various reasons. John Smith later published the vulnerability on the dark web, a place well known for trading computer viruses and other such malicious software/hardware. The Defendant files were downloaded subsequently by a hacker, Edward Snoward and were used to exploit Wayne Rooney's pacemaker. The Defendant did not have any knowledge of this activity. The attack involved more than just exploiting the vulnerability of the pacemaker. Edward Snoward performed thorough recon of the hospital's network and was able to successfully distract anybody monitoring the pacemaker by remotely manipulating the information in an effort to make things look normal. A fake pacemaker was subsequently installed by the hacker and the

pacemaker did not operate during Wayne Rooney's heart attack and caused his death. As a response, the family of Wayne Rooney filed charges against the Plaintiff of this case. On the grounds of unauthorized transfer of confidential data by the Defendant after leaving the company, whose rightful owner is the company alone, Heart2Heart would like to provide its defense to the Wayne Rooney's Family vs. Heart2Heart case.

In summary, we request the court to provide answers to the following questions:

1. Did the defendant violate his authorization to access company's data after departing the company?

2. Did the defendant not violate any legal implications by uploading valuable information belonging to Heart2Heart onto the dark web?

3. Did the implications of leaking vulnerability information ultimately cause the death of Wayne Rooney?

4. Did the Defendant cause further damage to the company and its consumers by acting on the basis of his own moral standards?

ARGUMENTS

A. The defendant violated Computer Fraud and Abuse Act (CFAA) and company policy in accessing the vulnerability information and keeping it in possession.

1. Evidence from the investigation carried out post Wayne Rooney's death clearly stated that the information the hacker Edward Snoward received was from an upload that was created by the Plaintiff.

2. The CFAA (18 U.S. Code § 1030) can be used here to prove Defendant's crime as the cost of the damages incurred from the vulnerability disclosure costed the Plaintiff well more than the $5000. These costs were incurred in compensating the victim's family, recalling all the devices that are in production and damage to brand reputation that resulted in loss of investors' interest in the company. All evidence required in order to prove these loses are available for scrutiny in front of the court.

3. The activities of the defendant also amply satisfies "furthering fraud by obtaining something of value" under CFAA Section (a)(4). The activities in this case has caused significant losses to intellectual property and brand reputation for the Plaintiff.

4. A person violates the CFAA act if he engages in "use and disclosure of all [database] information, except for legitimate Korn/Ferry business" (United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)). The plaintiff had clearly mentioned that any utilization of company's data except for company's need (in this case Heart2Heart) is a violation of the Employer's agreement. The

language of the statue clearly states the actions of the Defendant in leaking and uploading sensitive data had no relation to what was required for or by his Employer.

5. The Defendant's access was terminated as soon as he left the company but there was data that the Defendant held on to. Therefore, the plaintiff is also guilty as someone who used a computer 'without authorization' under 18 U.S.C §§ 1030(a)(2) and (4) when the person has not received any permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." (LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009)). In doing so, the defendant has **exceeded authorized access**.

B. Defendant made available the vulnerable code on an online market known for attracting potential hackers.

1. Stating back to an earlier evidence that came out of the investigation, the upload was proved to be made by the defendant on the dark web. This established fact forms the basis of this argument.

2. The defendant is guilty as he caused transmission of vulnerable code causing unauthorized damage to the pacemaker as per the United States v. Keys, No. CR. S-13-0082 KJM, 2014 WL 1232234 (E.D. Cal. Mar. 24, 2014)**.** The transmission was done with total knowledge of the legal implications the Defendant has to face. The CFAA act provides protection against such behavior as stated in CFAA sections 1030(a)(5)(A), "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." The defendant should be appropriately punished according to 1030(c)(4)(b) which states that "an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i)".

3. As a derivation of the above argument, the defendant is also guilty as per the provision of CFAA (**1030(a)(5)(A)** & **1030(b)**) which states attempting to transmit vulnerable code to cause unauthorized damage to a protected computer is against the law and "Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section". The validity of the above statute in this case is due to the various times the vulnerability details could have transferred over time since initial upload.

C. The case would be void and the pacemakers would be safe if not for the defendant's actions post his resignation from the plaintiff's company.

1. The tools and procedures required to discover this vulnerability is not publicly available and are proprietary pieces of technology belonging to the plaintiff's company. It could be argued that

vulnerabilities could be discovered by anybody outside the organization as well but it is to be noted that the computing power required to find this otherwise simple vulnerability to exploit are immense and expensive. This makes it finding any bugs in the software or in the pacemaker's hardware rare or not easy. This would have to be a state sponsored attack if any attacker wants to make such investments and gather the resources to find and exploit the vulnerability.

2. This is also a violation of the Employer's agreement of terms that state that "any theft or possession of data or asset that is of extreme value to the company will be liable to legal implications according to the state law. A major portion of the software code that was kept protected and locked away from normal users was exposed due to the vulnerability. This code controls a major portion of what the pacemaker is intended for. As a security measure during designing the produce, this portion of code was made to require the highest privileges to be viewed. This was obtained by obtaining a reverse shell into the pacemaker and performing privilege escalation to obtain "root" access. The defendant is therefore guilt of The Copyright Act as it gives copyright owners "exclusive rights ***to do and to authorize***" certain acts with respect to their copyrighted works, including "***to distribute copies*** or phonorecords of the copyrighted work to the public" 17 U.S.C. § 106(3) (emphasis added). "Anyone who violates any of the exclusive rights of the copyright owner as provided by section [] 106 . . . is an infringer of the copyright." 17 U.S.C. 501(a).

D. The Plaintiff's company took the necessary steps to protect the information it considered critical.

1. Human errors in software code is expected and cannot be avoided. It was important for the Plaintiff to consider how to avoid damages to both his employer and its customers and therefore take a mutually agreeable decision favoring both parties. A lot of the plaintiff's customers would have to also go through considerable effort to get another pacemaker and considering the criticality of a pacemaker, such incidents are not desirable.

2. The expensive nature of finding these vulnerabilities were the Plaintiff's security guarantee that was relied on. This is not uncommon in the world of computer security, as an example, a lot of cryptographic algorithms are considered to be unbreakable as they have a very low mathematical probability of causing a valid attack.

3. The Defendant's employer took all the necessary steps to avoid a compromise of the security of his product as a part of manufacturer's responsibility to overall product quality. Employment agreements with specific details about handling of data for company's purposes were mentioned and signed by the Defendant as a part of his onboarding process. A failure to comply with these agreements is a simple violation of the Employer's policy. As a continued security measure, the company also took steps to file a DMCA takedown report as soon as the incident came to light. The website has been since been taken down but the extent of damages that the Plaintiff will

have to incur is a difficult prediction considering the extent to which the software code could have been distributed over the Internet and other communication mediums.

CONCLUSION

The arguments presented by the Plaintiff cover several aspects of the information leak and provide the necessary details to support their stand. The Defendant has been conclusively found to be responsible for keeping information of value to the Employer and later transferring the information to dark web. The Defendant caused additional damage to the Plaintiff's as a result of misjudgment on his part. It should be in this case, irrelevant to take into consideration the intention of the Defendant (whether "good" or "bad") in publishing the vulnerability online.

In summary, there are various violations that the Defendant committed that have led to a series of events leading upto the victim's death. The Defendant did not choose to settle this matter internally with the necessary persistence that would be expected in an issue where the Plaintiff and the Defendant have conflicting opinions of a situation. The Plaintiff was not made aware of any of the actions that the Defendant took.

For all those reasons, the Plaintiff requests (1) an order that authorizes him to penalize and recover compensatory damages under the CFAA (2) an injunction as prayed for in Plaintiffs' Complaint preventing Defendants from further copyright infringement, (3) Hold the Defendant acts as fully responsible for the victim's death, (4) Impose fines for copyright infringement as per the copyright act and help in establishing the right message, and Plaintiffs further request such other relief as the Court deems just and necessary.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on April 26, 2018, a copy of the foregoing document was served upon the Defendants via United States Mail at the following address:

John Smith

4192 N. 81st Street

Scottsdale, Az 85251-2672

Plaintiffs

__CEO, Heart2Heart_____