Steven Cheng, Prashanth Venkateswaran , Sagar Wani , Venkata Aditya Bollapragada, Patrick Collins, Chanakya Gaur

Law and the Internet

7 March 2018

Fact Pattern

A pacemaker works by detecting the heart rate of the heart the device is attached to and generates an small electrical pulse to make the heart beat at a regular pace. Normally when the device is initially installed, the pacemaker is connected to the hospital network so that it can be monitored and the hospital can be sure that the device is working as expected. A company called *Heart2Heart* produces pacemakers for patients who recently had a heart attack and has irregular heartbeats. In developing their pacemaker, *Heart2Heart* unknowingly built it insecurely and after distributing their product, they later realized that a huge flaw had been built into their system that would allow a motivated hacker to disrupt normal operation. The technicians at the company knew about the security flaw in their design and were working on a fix, but did not produce a fix fast enough to be released in the current models. A patient at the Maryland Hospital, Wayne Rooney, needed to have pacemaker installed and received the pacemaker built by *Heart2Heart.* While at the hospital, a hacker known as Eden Snoward hacked the hospital network and exploited the vulnerability built in the pacemaker, causing the signals that are produced when a heart attack happens to look like normal heart beats. The patient, Wayne Rooney, then had a heart attack and the pacemaker did nothing to stop it and he died. Rooney's family finds out that the company, *Heart2Heart*, did know about the vulnerability but still yet chose to put their product out on market.

After an investigation about the cause of the attack was launched, it was determined that the attacker had first infiltrated the hospital network, intercepted the traffic between the

pacemaker and the hospital, and set up a fake pacemaker to trick the hospital into thinking that the fake pacemaker was Rooney's pacemaker. The attacker could then forge his own data to send to the hospital and they would believe it was from Rooney's pacemaker. In addition, the attacker took advantage of the vulnerability in the firmware to achieve a reverse shell, essentially allowing the attacker to send any commands to the device itself. With the reverse shell, the attacker was able to kill all electrical pulses generated by the device. Later on, Rooney had a heart attack at the hospital and the pacemaker did not generate the electrical pulse it was supposed to generate. The hospital also did not receive any alerts that Rooney was experiencing a heart attack. Because there were no alarms, his heart attack went unnoticed and he died.

It was also later discovered that the attacker had received the information about the vulnerability on the dark web. The source of the information was an ex-employee of the company *Heart2Heart* who knew about the vulnerability during development. His employment was terminated because he kept pressuring the company to halt production until a fix was produced. Frustrated with this company, he went to the dark web to expose *Heart2Heart* for its malpractice.

The prosecutor in this case is the family of Wayne Rooney and they are suing *Heart2Heart* for medical negligence and producing a product with a vulnerability that could lead to death.