

Cyber Crime Report

Sam Roethemeyer

University of Advancing Technology

## Cyber Crime Report

On September 19, 2016, in Hamilton Ohio, Ross Compton aged 59, made a call to the fire department stating that he awoke to his house ablaze. He stated that when he woke up, he packed a few clothes and busted through the window of his house with his cane and jumped out. He also told the ambulance that arrived that he had a pacemaker. With this knowledge, the police then acquired a search warrant for the pacemaker data that is recorded and can be retrieved for analysis. It was determined by a cardiologist that it was “highly improbable” that he was able to collect his things, break his window, and jump out because of his medical conditions. The statements he gave the authorities were also inconsistent with this data because it showed that there were cardiac rhythms before, during, and after the events stated. The search warrant was granted by the judge because of gasoline discovered on his clothes at the time.

If the gasoline had not been discovered, then there would have been no investigation into the fire. Ross also messed up when he told the authorities that he had a pacemaker, because then they can access the data recorded from his pacemaker that shows his statements were inconsistent with the data acquired from said pacemaker.

His attorney pleaded not guilty with reason of insanity. He was indicted in January of 2018 following a psychological evaluation. Allegedly the defendant reportedly has had a history of mental illness. The psychological evaluation ruled him competent for the trial and to be able to assist his defense. He was reportedly non-compliant in his treatment for over 5 months.

This case raised concerns on privacy over personal and medical information in the digital world. It is one of the first of its kind because of the use of his pacemaker as evidence against

him. The attorney wanted the pacemaker evidence thrown out because it invaded his constitutional rights and unreasonable seizure of his private information. The acquirement of the pacemaker information was viewed similarly as how blood samples are when using a warrant to get the information from the hospital. Since the information was sent to the hospital, it wasn't his private information since it was now a part of his medical records. Authorities are still able to get warrants for devices such as smart watches and smart home devices such as Google home and Amazon echo. Authorities don't view data differently no matter where it is, inside or outside of the body. This is why there is large concern over this case. If you have no choice to get a pacemaker, why should your data now be considered not yours over people who don't have pacemakers that store data. If we must get a device that is essential to our survival, why is the data that it collects treated as public information vs someone who doesn't have the device.

## References

- JurisMagazine, & Written by JurisMagazine. (2017, April 2). *'telltale heart': Evidence found in defendant's cardiac pacemaker contains incriminating evidence of arson*. Juris Magazine. Retrieved October 7, 2021, from [https://sites.law.duq.edu/juris/2017/04/02/telltale-heart-evidence-found-in-defendants-cardiac-pacemaker-contains-incriminating-evidence-of-arson/#\\_ftn8](https://sites.law.duq.edu/juris/2017/04/02/telltale-heart-evidence-found-in-defendants-cardiac-pacemaker-contains-incriminating-evidence-of-arson/#_ftn8).
- Paul, D. (2017, July 29). *Your own pacemaker can now testify against you in Court*. Wired. Retrieved November 12, 2021, from <https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/>.