

State of Ohio v. Ross Compton: Internet-enabled medical device data introduced as evidence of arson and insurance fraud

The International Journal of
Evidence & Proof

2020, Vol. 24(3) 321–328

© The Author(s) 2020

Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/1365712720930600

journals.sagepub.com/home/epj



Marie-Helen Maras 

John Jay College of Criminal Justice, NY, USA

Adam Scott Wandt

John Jay College of Criminal Justice, NY, USA

Abstract

The data generated by Internet of Things devices is increasingly being introduced as evidence in court. The first US case involving the introduction of medical data from a pacemaker as evidence of arson and insurance fraud was *State of Ohio v Compton*. The purpose of this article is three-fold. First, the article explores this case, looking in particular at the facts of the case and the charges brought against the defendant. Second, the article critically examines the decision of the trial court judge during the suppression hearing for the evidence from the pacemaker. In this hearing, the judge ruled that the search and seizure did not violate the Fourth Amendment rights of the defendant and allowed the pacemaker data to be entered as evidence against him. Third, the article considers the implications of this decision for future cases involving Internet-of-Things (IoT) medical data. Ultimately, the constitutional protections of IoT medical device data and the circumstances under which the data from these devices will be collected and used as evidence, are issues that currently demand the attention of legal and digital forensics professionals and warrant public debate.

Keywords

Arson, insurance fraud, Internet of things, pacemaker, right to privacy

Corresponding author:

Marie-Helen Maras, John Jay College of Criminal Justice, 524 W 59th St, New York, NY 10019, USA.

E-mail: mmaras@jjay.cuny.edu

The Internet-of-Things (IoT) is a term used to describe the connection of everyday objects to the Internet in order to enable the real-time and remote monitoring of property, people, plants and animals, and the vast collection, storage, use and transfer of data about them, in order to provide owners and users of the device with a service (Maras, 2015). Even medical devices, such as pacemakers and defibrillators, have become part of the IoT. IoT medical devices were created to improve efficiency and quality of life, and provide everyday conveniences to the user. These devices collect, store and share significant quantities of personal and health data about the user.

Data from IoT devices can be (and have been) introduced as evidence of a crime, serve as an alibi and support and/or refute the testimony of witnesses, victims and suspects (Maras and Wandt, 2019; Maras, forthcoming). For example, data from an IoT wearable device, FitBit, which measures and monitors physical activity, exercise and sleep patterns, has been used to refute an allegation of sexual assault and has been admitted as evidence in murder trials (Dancyger, 2018; Lartey, 2017; Privacy International, 2019; Smiley, 2019; Syder, 2015). In 2017, data from a medical device was introduced in a case as evidence of a crime and to refute the testimony of the suspect, Ross Compton. Particularly, in *State of Ohio v Ross Compton*,¹ for the first time, data from an IoT medical device—an implanted pacemaker—was used to charge the defendant with arson² and insurance fraud.³

Facts of the case

In September 2016, 59-year-old Ross Compton reported a fire to the alarm company after the company called him to inquire about a loss of power in the home.⁴ Compton instructed the company to contact 911 (the emergency telephone number for the United States) and report the fire.⁵ First responders were dispatched to Compton's home. Compton informed authorities that he woke up in the middle of the night to find his house was on fire, hastily collected his belongings, broke the window, threw his belongings out of the window and exited his home.⁶

The investigation

The investigation of the fire revealed that fires originated from multiple locations in the house and traces of gasoline were found in the home pointing to arson.⁷ Investigators also found traces of gasoline on Compton's clothes and shoes.⁸ The investigation further revealed that Compton had a medical condition, requiring the use of an 'external heart pump . . . and implanted cardiac pacing device (i.e., pacemaker).'⁹ Given Compton's medical condition, the timeline of events that Compton provided were deemed 'highly improbable' by a cardiologist.¹⁰ Due to inconsistencies in Compton's story and the evidence obtained from the arson investigation, a search warrant was sought and obtained in October 2016, for Compton's cellphone and data from his pacemaker.¹¹ Pursuant to the search warrant, Compton was compelled to go

-
1. *State of Ohio v Ross Compton*, Case No. CR 2016-12-1826.
 2. Compton was charged with aggravated arson pursuant to § 2909.02(A)(2) of the Ohio Revised Code, which holds that '[n]o person, by means of fire or explosion, shall knowingly . . . [c]ause physical harm to any occupied structure'.
 3. Compton was charged with insurance fraud pursuant to § 2913.47(B)(1) 'any written or oral statement that is part of, or in support of, an application for insurance, a claim for payment pursuant to a policy, or a claim for any other benefit pursuant to a policy, knowing that the statement, or any part of the statement, is false or deceptive' with the intention of defrauding or knowingly facilitating fraud.
 4. *Compton*, above n. 1 at 2 (Motion to Suppress, 5 May 2017).
 5. *Compton*, above n. 1.
 6. *Compton*, above n. 1. See also Wootson (2017).
 7. *Compton*, above n. 1 at 21 and 54–55 (Suppression Hearing, 11 July 2017).
 8. *Compton*, above n. 1.
 9. *Compton*, above n. 1 (Motion to Suppress).
 10. *Compton*, above n. 1.
 11. *Compton*, above n. 1 (Suppression Hearing)

the Atrium Medical Center so the data produced by his pacemaker, which revealed Compton's cardiac activity, could be seized by law enforcement.¹²

A violation of the right privacy?

Compton's defence argued that the search and seizure of the pacemaker data violated Compton's constitutional right to privacy. The right to privacy is not explicitly mentioned in the United States Constitution. However, the Fourth Amendment to the US Constitution does implicitly refer to the right to privacy:

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

US jurisprudence on the Fourth Amendment reveals vacillating perspectives of this right: (1) the Fourth Amendment is a property-based right, applying to the protection of personal property from intrusions (i.e., trespass);¹³ (2) the Fourth Amendment is a privacy-based right, rejecting the need for physical intrusions to be present, applying instead to the person and determinations of reasonable expectations of privacy.¹⁴ The Court of Common Pleas¹⁵ (hereafter trial court) in Butler County, Ohio, where Compton's suppression hearing occurred, followed a privacy-based analysis of the Fourth Amendment. For Fourth Amendment protections to apply, a search or seizure must have occurred and the government (or someone acting as an agent of the government) must have conducted the search or seizure. In Compton's case, a government search was established and was not a contested issue in the hearing. What was contested was whether the search complied with the requirements of the Fourth Amendment—that is, whether the search warrant was valid and the search and seizure was constitutional.¹⁶

Validity of the search warrant

Pursuant to the Fourth Amendment, a search warrant, which is supported by probable cause and is sufficiently particular in the places and items to be seized pursuant to this warrant, is needed (Maras, 2014). US jurisprudence reveals that search warrants are required when bodily evidence (e.g., blood, urine, DNA, hair samples and saliva) is sought,¹⁷ with a few exceptions.¹⁸ Digital data is also obtained

12. *Compton*, above n. 1 at 3 (Motion to Suppress).

13. Here, physical (and even non-physical) intrusions into constitutionally protected areas and into and on human bodies constitute a 'search' (e.g., home, biological material, GPS tracking on vehicle, and GPS trackers worn on bodies). See, for example, *Olmstead v United States*, 277 US 438 at 465 (1928) (physical intrusions into constitutionally protected areas); *United States v Jones*, 565 US 400 (2012) (the 'attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment'); and *Grady v North Carolina*, 135 S. Ct. 1368 at 1369–1370 (2015) (a state 'conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movement').

14. Searches are associated with 'people, not places'. *Katz v United States*, 389 US 347 at 351 and 353 (1967).

15. This is the lowest level trial court of general jurisdiction that hears both civil and criminal cases and is authorised to hear felony cases in Ohio. Cases litigated in the Court of Common Pleas are subject to appellate review by the appropriately districted Ohio Court of Appeals. Cases appealed further would require certiorari granted by the Ohio Supreme Court. See Butler County (2020) for more information about the judicial structure in Ohio.

16. *Compton*, above n. 1 at 3 (Motion to Suppress).

17. See, for example, *Schmerber v California*, 384 US 757 (1966); *Graves v Beto*, 400 US 960 (1970); *Skinner v Railway Labor Executives' Association*, 489 US 602 (1989); *State v Thompson*, 886 NW 2d 224 (Minn 2016); *Raynor v State*, 99 A.3d 753 (Md 2014).

18. Certain US courts have not applied this general rule for bodily evidence obtained via so-called minor intrusions, such as the taking of hair samples. See, for example, *United States v D'Amico*, 408 F.2d 331 (2d Cir 1969); *State v McCumber*, 622 P.2d 353 (Utah 1980); and *United States v Weir*, 657 F.2d 1005 (8th Cir 1981).

pursuant to a search warrant. In fact, search warrants have been used to access and collect private personal information from suspects, such as data from cars' black boxes that include information about drivers and data from computer devices, smartphones and other forms of technological devices.¹⁹

In Compton's case, a legal order (i.e., search warrant) was obtained before information was collected from his pacemaker.²⁰ Compton's defence team questioned the validity of the search warrant in a motion to suppress evidence obtained from Compton's pacemaker and other related medical information.²¹ Following the defendant's motion to suppress evidence, the trial court conducted a suppression hearing in accordance with Rule 12(C)(3) of the Ohio Rules of Criminal Procedure. During this hearing they applied the relevant bipartite Fourth Amendment test based upon the traditional standard used to suppress evidence seized in violation of the Fourth Amendment.²² The first prong of the applied standard is whether there was probable cause in the affidavit to warrant the granting of the search warrant. During the suppression hearing, the judge ruled that there was sufficient probable cause to issue a search warrant for the pacemaker data.²³ Specifically, the court concluded that there was probable cause in that the 'information in the pacemaker would be useful in getting . . . information [relating to the timing of the fire and verifying Compton's story] to the investigators.'²⁴ Accordingly, the judge deemed that the search warrant was validly issued.

Constitutionality of the search and seizure

In their motion to suppress evidence, Compton's defence team argued that the State conducted 'an unreasonable search and seizure' of Compton's private information. The second prong of the standard used to suppress evidence in violation of the Fourth Amendment applies to the actual information the government is seeking. Here, 'even if there was probable cause' the court examines if the 'warrant, or the execution of the warrant [goes] beyond what it should be allowed to go to protect the right of privacy . . . of the [d]efendant.'²⁵ Compton's defence team argued that the specific information sought (pacemaker records) were private and releasing the information would violate the defendant's right to privacy.²⁶

US case law regarding searches and seizures of evidence from the human body reveals that the constitutionality of government action in this regard depends on the 'reasonableness' of the search and seizure.²⁷ On this matter, US courts have engaged in a case-by-case evaluation of reasonableness, considering the totality of the circumstances in each case.²⁸ For instance, in *United States v Crowder*, where the bodily evidence was a bullet that was surgically removed from the defendant's arm, the court considered the following factors when rendering its decision:

- (1) the evidence sought was relevant, could have been obtained in no other way, and there was probable cause to believe that the operation would produce it; (2) the operation was minor, was performed by a skilled surgeon, and every possible precaution was taken to guard against any surgical complications, so that the risk of permanent injury was minimal; (3) before the operation was performed the District Court held an adversary hearing at which the defendant appeared with counsel; (4) thereafter and before the operation was performed the defendant was afforded an opportunity for appellate review by this court.²⁹

19. *State v Worsham*, 227 So.3d 602 at 604, 606 (Fla Dist Ct App 2017); *Riley v California*, 134 S. Ct. 2473 (2014); Maras (2014).

20. *Compton*, above n. 1 at 54–55 (Suppression Hearing).

21. *Compton*, above n. 1 at 2–5 (Motion to Suppress).

22. *Mapp v Ohio*, 367 US 643 (1961).

23. *Compton*, above n. 1 at 54–55 (Suppression Hearing).

24. *Compton*, above n. 1 at 55.

25. *Compton*, above n. 1.

26. *Compton*, above n. 1 at 56.

27. *Breithaupt v Abram*, 352 US 432 (1957); *Samson v California*, 547 US 843 at 848 (2006).

28. See, for example, *Schmerber v California*, above n. 17; *Winston v Lee*, 470 US 753 (1985).

29. *United States v Crowder*, 543 F.2d 312 (DC Cir 1976).

In *Breithaupt v Abram* and other US cases, the court recognised the need to balance competing personal privacy interests and law enforcement interests with respect to public safety and public policy.³⁰ In evaluating the reasonableness of searches and seizures, US courts examine the manner in which the search was conducted.³¹ Here, the ‘intrusiveness’ of the procedure to obtain evidence from the human body is examined. In *Winston v Lee*, to assess ‘intrusiveness’, the court evaluated both the medical risk and the potential adverse impact of the procedure on the human dignity of the defendant. For example, a determination is made as to whether the search procedure was minimally invasive or noninvasive, and was conducted as part of a safe and routine practice.³² In Compton’s case, the judge found that the procedure was not overly intrusive or invasive given that the data was retrieved using a non-invasive procedure.³³ Specifically, to retrieve the data, a technician uses a hand-held device to identify the implant and initiate data retrieval (i.e., to ‘interrogate’ the implanted medical device) without touching the person, often over the person’s clothes.³⁴ US case law further reveals that courts examine the probative value of the evidence sought.³⁵ The court transcript of the suppression hearing revealed that the device used to collect data from Compton’s pacemaker contained a sensor that detected patient movement (i.e., ‘movement ticks’).³⁶ The ‘movement ticks’ along with corresponding heart rate data, was considered critical evidence in this case because it contradicted Compton’s claim that he was asleep at the time the fire started.³⁷ For these reasons, the defendant’s motion to suppress the information seized from his pacemaker was denied by the court. The judge not only found that the search and seizure was reasonable, the judge also concluded that the collection of heartbeat data and its introduction as evidence in a court of law, when considering other forms of personal data, was ‘just not that big of a deal’.³⁸

What this means for future cases

In the United States, information provided to third parties is not protected by the Fourth Amendment. Specifically, in *Smith v Maryland*,³⁹ the court ruled that there is no legitimate expectation of privacy of information voluntarily revealed to a third party (i.e., the third-party doctrine).⁴⁰ However, in Compton’s case, the pacemaker information sought in the search warrant ‘only exists because [Compton] has a unique medical condition . . . and . . . [his pacemaker] provides information to his doctor so his doctor can keep him alive.’⁴¹ In light of this, how ‘voluntary’ is the provision of this information to a third party? In *United States v Jones*, Justice Sotomayor questioned the third party-doctrine in today’s technology-dependent world by stating, ‘it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.’⁴²

30. *United States v Crowder*, above n. 29 at 439–440.

31. *Rochin v California*, 342 US 165 (1952); *Breithaupt v Abram*, 352 US 432 (1957); *Schmerber v California*, above n. 17; and *Winston v Lee*, above n. 28.

32. Above n. 29.

33. *Compton*, above n. 1 at 65 (Suppression Hearing).

34. *Compton*, above n. 1 at 40 and 65.

35. *Winston v Lee*, above n. 28 at 762–763.

36. *Compton*, above n. 1 at 41 (Suppression Hearing).

37. *Compton*, above n. 1 at 41–42.

38. *Compton*, above n. 1 at 66.

39. 442 US 735 (1979).

40. The notion that there is no legitimate expectation of privacy in information voluntarily revealed to a third party was recently readdressed by the US Supreme Court in *Carpenter v United States*, 819 F.3d 880 (6th Cir 2016). In *Carpenter*, the court held that law enforcement must have a valid search warrant to request historical geolocation information from a suspect’s smartphone cellular provider.

41. *Compton*, above n. 1 at 61 (Suppression Hearing).

42. *United States v Jones*, above n. 13 (Sotomayor, J., concurring).

Given that incriminating evidence was obtained from Compton's pacemaker, an important question to consider is whether the production of this incriminating data violates his Fifth Amendment rights. The Fifth Amendment to the US Constitution holds that:

[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

The applicable part of this right to Compton's case is its inclusion of a privilege against self-incrimination (i.e., 'no person . . . shall be compelled in any criminal case to be a witness against himself'). In *Fisher v United States*, the Court held that the Fifth Amendment only 'protects against "compelled self-incrimination, not [the disclosure of] private information".'⁴³ US jurisprudence reveals that the Fifth Amendment 'offers no protection against compulsion to submit to fingerprinting, photography, or measurements, . . . to appear in court, to stand, to assume stance, to walk, or to make a particular gesture'⁴⁴ because this does not require the communication of knowledge by the defendant.⁴⁵ For the same reason, the prohibition against self-incrimination does not apply to the use of evidence obtained from a suspect's body (e.g., blood, saliva, or voice exemplar) when it may be material to the case.⁴⁶ In view of that, the compelled act in Compton's case, which is the production of data from his pacemaker (even if incriminating), would not be considered a violation of his Fifth Amendment rights according to existing case law. Nevertheless, while Compton's defence team did not claim that the compelling of the pacemaker data violated his Fifth Amendment rights, future defendants under the similar circumstances may attempt to argue that the information held within their pacemakers constitute electronic testimonial evidence. Beyond the constitutional issues that Compton's case raises, if the introduction of evidence from these devices in court becomes more commonplace, people may be less likely to use life-saving devices if they fear that the data collected by them could or would be used against them.

Following the Compton case, law enforcement authorities in Ohio sought and retrieved IoT medical device data (i.e., from pacemakers) in two murder cases.⁴⁷ The introduction of IoT medical device data and IoT health data as evidence in court is not limited to the United States. For example, in the United Kingdom and Germany, iPhone health data and other health app data have been introduced as evidence in sexual assault and murder cases (Privacy International, 2019). As medical technology advances, implanted IoT medical devices will become more commonplace (Taylor et al., 2018). These devices contain onboard memory storage that is populated by sensors and other forms of data input. Information on these devices will most certainly be considered private by its users, while being of interest to law enforcement and others. Medical data, irrespective of where it is stored and the manner in which it is accessed (physical or remote), warrants constitutional protection because it reveals personal, intimate health and medical information (Draft, 2019: 540). The United States Supreme Court has recently expanded protections given to users of smartphones.⁴⁸ An expansion of constitutional protections involving implanted medical or technical devices may also be necessary. The introduction of IoT

43. *Fisher v United States*, 96 S. Ct. 1569 (1976). See also *Schmerber v California*, above n. 17 at 761.

44. *Schmerber v California*, above n. 17 at 764; *United States v Wade* 388 US 218 (1967) at 223.

45. *Virginia v Baust*, No CR14-1439 (Va Cir 28 October, 2014) at 3.

46. *Holt v United States*, 218 US 245 at 252–253 (1910); *Schmerber v California*, above n. 17; *US v Dionisio*, 410 US 1 (1973); *People v Smith*, 86 AD.2d 251 at 252 (NY App Div 3d Dept 1982).

47. *State of Ohio v Douglas Best*, Case No CR 2017-01-0025 (Plea of Guilty and Jury Waiver, 4 October 2017); *State of Ohio v Charles Ray Graham*, Case No CR 2017-01-0026; see also Police Professional (2017).

48. *Riley v California*, above n. 19.

medical device data as evidence in courts is occurring with greater frequency both within and outside of the United States. How the information from IoT medical devices will be made available, used in courts nationally and internationally, and under what circumstances the data from these devices will be collected and used as evidence, are issues that currently demand the attention of legal and digital forensics professionals and warrant public debate.


Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The authors would like to thank the John Jay College of Criminal Justice Center for Cybercrime Studies for the funding to obtain the court transcripts needed to analyze this case.

ORCID iD

Marie-Helen Maras  <https://orcid.org/0000-0003-3428-4622>

References

- Butler County, Ohio Common Pleas Court (2020) The Judicial Structure in Ohio. Available at: www.bccommonpleas.org/about_us/ohio_judicial_structure.php (accessed 13 May 2020).
- Dancyger L (2018) Fitbits are snitching on criminals—here’s how. *Rolling Stone Magazine*, 4 October. Available at: www.rollingstone.com/culture/culture-news/fitbit-apple-watch-crime-help-solve-733050/ (accessed 13 May 2020).
- Draft AE (2019) Pacemakers, Fitbits, and the Fourth Amendment: Privacy implications for medical implants and wearable technology. *Michigan State Law Review* 2: 511–553.
- Lartey J (2017) Man suspected in wife’s murder after her Fitbit data doesn’t match his alibi. *The Guardian*, 25 April. Available at: www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate (accessed 13 May 2020).
- Maras M-H (2014) *Computer Forensics: Cybercriminals, Laws and Evidence*. 2nd edn. Burlington, MA: Jones and Bartlett.
- Maras M-H (2015) The Internet of Things: Security and privacy implications. *International Data Privacy Law* 5(2): 99–104.
- Maras M-H (forthcoming) *Cyberlaw and Cyberliberties*. Oxford: Oxford University Press.
- Maras M-H and Wandt AS (2019) Enabling mass surveillance: Data aggregation in the age of Big Data and the Internet of Things. *Journal of Cyber Policy* 4(2): 160–177.
- Police Professional (2017) The tell-tell heart. Available at: www.policeprofessional.com/news/the-tell-tell-heart/ (accessed 13 May 2020).
- Privacy International (2019) IoT in Court. Available at: <https://privacyinternational.org/campaigns/iot-court> (accessed 24 October).
- Taylor K, Steedman M, Sanghera A, et al. (2018) *Medtech and the Internet of Medical Things: How Connected Medical Devices are Transforming Health Care*. London: Deloitte Centre for Health Solutions. Available at: <https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html> (accessed 13 May 2020).
- Smiley L (2019) A brutal murder, a wearable witness, and an unlikely suspect. *Wired Magazine*, 17 September. Available at: www.wired.com/story/telltale-heart-fitbit-murder/ (accessed 13 May 2020).

- Syder M (2015) Police: Woman's fitness watch disproved rape report. ABC News, 19 June. Available at: <http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/> (accessed 13 May 2020).
- Wootson Jr CR (2017) A man detailed his escape from a burning house. His pacemaker told police a different story. *The Washington Post*, 8 February. Available at: www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/ (accessed 13 May 2020).