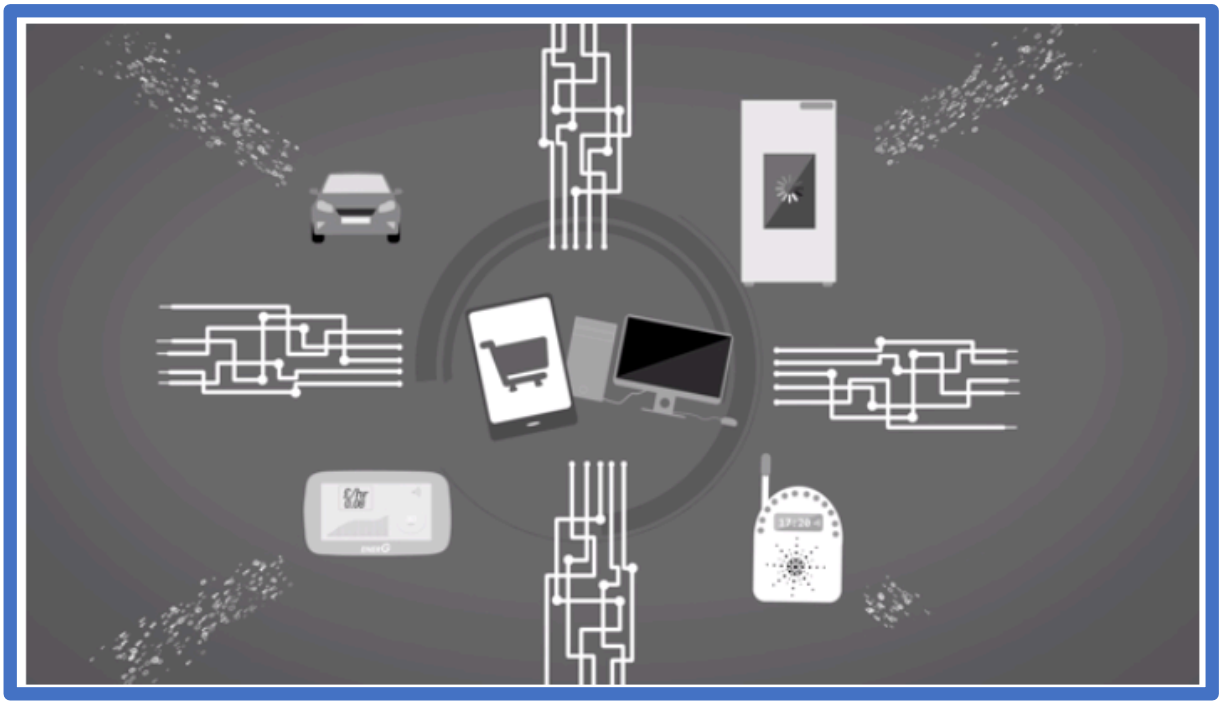
With my fridge as my witness?!



Everyday objects and devices that can connect to the Internet -- known as the Internet of Things (IoT) or connected devices -- play an increasing role in crime scenes and are a target for law enforcement. Exploiting new technologies that are in our homes and on our bodies as part of criminal investigations and for use as evidence, raises new challenges and risks that have not been sufficiently explored.

We believe that a discussion on the exploitation of IoT by law enforcement would benefit from the views of a wide spectrum of voices and opinions, from technologists to criminal lawyers, forensic experts to civil society. Here we set out some initial concerns.

PRIVACY INTERNATIONAL

What is the problem?

Our world is full of devices and objects that connect to the internet[i]. From household items such as doors, lightbulbs, hairbrushes, hoovers and lawn mowers, to wearables such as watches, Fitbits, and earphones and more complex objects such as cars. These so-called smart objects can collect intimate data using sensors, microphones and cameras not only about our everyday lives but those of our family and friends.

As shown in Figure 1, dissection of a Nest Thermostat, sensors can include temperature, humidity, light, ultrasound, compass, accelerometer, gyroscope and GPS receivers.

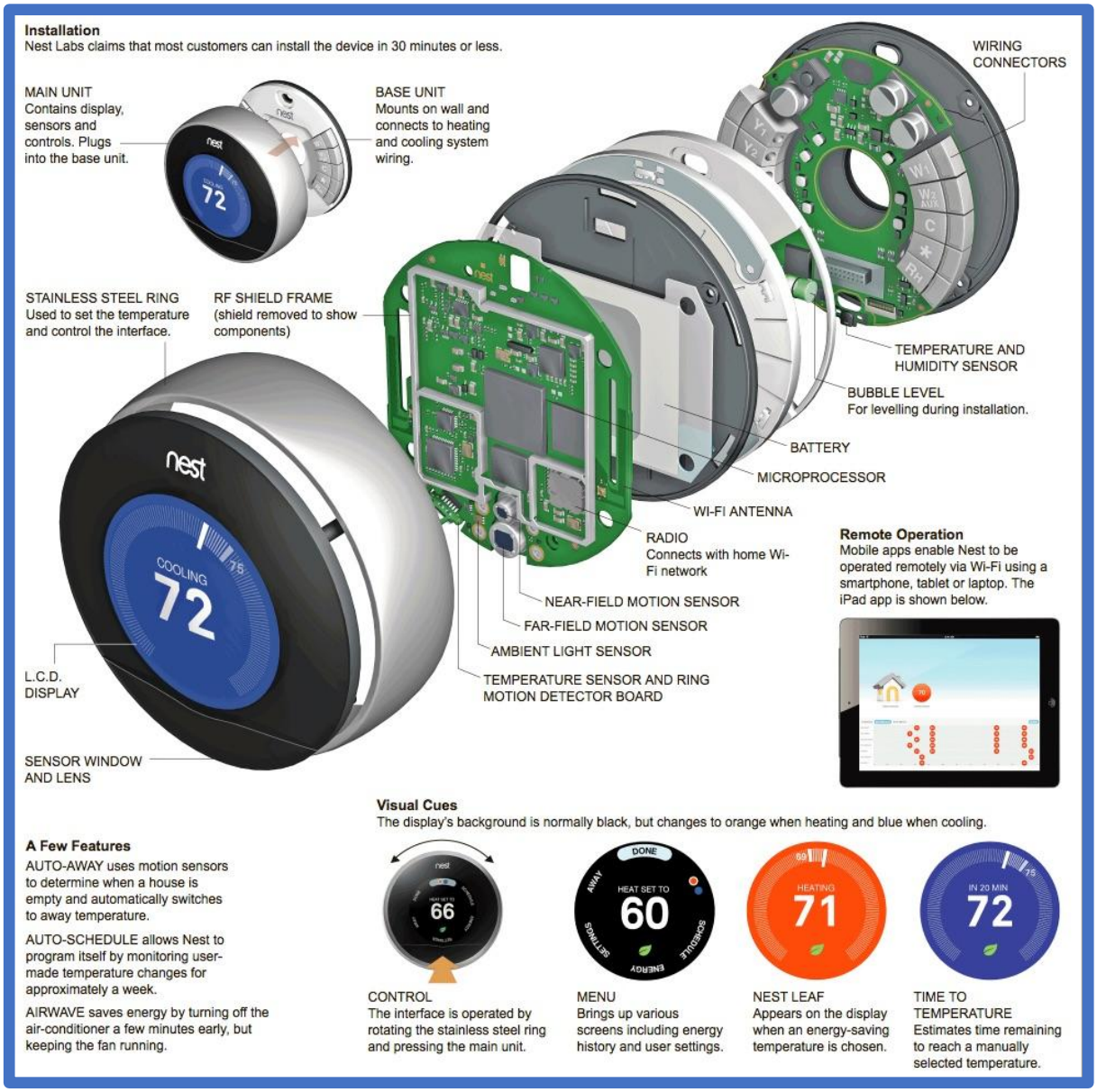


Figure 1: From: NYTimes infographic Inside the Nest Learning Thermostat

We have little understanding of the capabilities of these devices and often do not realise how insecure they are. Barbie's connected-smart doll released in 2015 came equipped with a microphone, voice recognition software and artificial intelligence that allowed a call-and-response function between the child user and the doll[ii]. The Norwegian Consumer Council reported in December 2016 that "Children are especially vulnerable when it comes to connected devices" noting in their review of toys, serious issues including lack of security, illegal user terms, kids' secrets being share and kids being subject to hidden marketing.

Figure 2: "Connected toys violate European consumer law", Forbrukerrådet, 6 December 2016, available at https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/.

A smart light bulb, just through collecting and analysing when it is turned off and on, can learn household behaviours. In 2017 it was reported that whilst vacuuming your home, Roomba 980's sensors could report on the size of a home and amount of furniture[iii]. We are often ignorant of the capabilities of the devices that surround us because, like the microphone in Google's Nest Secure, they are kept secret.[iv]

The digital witness

As these devices proliferate and permeate our every day, little thought has been given to the implications of one particular use of the data collected by sensors, actuators and microphones: this data is sought and used by the government in criminal investigations and as evidence in criminal proceedings. The digital "witnesses" that will acquit us or convict us.

In most instances these devices may not by themselves be the critical piece of evidence that could result in acquittal or conviction. A more common circumstance is likely to be that they will play some role, lead to some other piece of evidence, be used to corroborate or contradict other evidence, to support or discredit a witness.

Intelligence and law enforcement agencies have begun to consider how the data these devices collect, and store can inform investigations and prosecutions. The National Security Agency (NSA) of the United States of America has already been exploring potential uses of

internet-connected devices, including biomedical devices such as pacemakers and insulin pumps to monitor individuals[v]. The UK Home Office informed Privacy International that they plan to develop skills and capacity to exploit the Internet of Things as part of criminal investigations[vi]. In January 2017 Scotland Yard digital forensic chief Mark Stokes declared that the 'Internet of Things' devices are likely to revolutionise crime-scene investigation.[vii]

What are the implications?

We are fascinated by the role of devices in criminal investigations but have failed to look beyond the headlines to critique what this means for society and peoples' rights to a fair trial, privacy, and other human rights that privacy supports. When prosecutors sought evidence during the criminal investigation of James Bates, which they believed was stored on Amazon servers via use of an Amazon Echo, people were ready to opine on Amazon's role, but little was said about what it means for connected devices to become a silent witness.

In November 2015, Bates had friends over at his house to watch football. In the morning, one of his friends was found dead in the hot tub.[viii] Police in Bentonville, Arkansas, issued a warrant to Amazon, asking Amazon to hand over any data that may have been recorded by the suspect's Echo speaker[ix]. Bentonville police served two search warrants ordering Amazon to turn over "electronic data in the form of audio recordings, transcribed records, text records and other data contained on Amazon Echo device" belonging to James Bates. Bates's attorney at the time, Kimberly Weber stated the court orders were "vague and full of supposition." Amazon stated it "objects to overbroad or otherwise inappropriate demands as a matter of course."[x]. Lawyers for Amazon filed a motion stating:

'*Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials. Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course.*'

The dispute ended when the suspect himself stated he would voluntarily hand over the data to the police. Amazon then turned over the recordings later the same day[xi].

In November 2017 an Arkansas judge acceded to the prosecution's application to dismiss the murder charge against Bates.

The spectrum of problems presented by connected devices, from issues of data protection, consumer protection and the shady data broker industry are ones where Privacy International is actively engaged to seek change.[xii]

The challenges presented by the toothbrush that knows your location[xiii] or the smart mattress that logs your bedtime activities[xiv], being used to investigate and prosecute you are ones that lack scrutiny and are likely to be accompanied by outdated legal procedures.

Information asymmetry

In criminal investigations, it is likely that the police will have access to more information and better tools than the witness, victim or suspect. In civil litigation it is also often the case that one party is at a financial and resource advantage compared to the other, whether it be the State or a wealthy individual or company. This is not a unique issue related to digital evidence. Individuals generally do not have the expertise to analyse, for example, physical or biological evidence such as fingerprints, shoe impressions, fibres, blood or saliva in the same way they would not have the skills to extract and interpret digital evidence. We explore issues around expert evidence and unequal access to justice below.

However, there is something about the nature of connected devices which makes the information asymmetry at the very least, uniquely unsettling. Particularly when you draw in debates around the skills of those interrogating devices and what a victim, witness or suspect may not realise about the capabilities of the devices they bring into their homes or work.

Devices log, process and transfer vast amounts of data about some of the most intimate parts of our everyday lives. The owner of a device may not know what data the device collects, shares and stores. Whilst some data may be visible to the user via a screen interface, a large amount, particularly that which is sent to third party servers (i.e. Cloud storage) is largely invisible. For example, a sex toy company was sued for secretly collecting intimate details without the user's knowledge[xv]. The device registered and sent to the company logs as to when the device was used and what intensity setting the user selected.

As users, we do not know the full range of data that connected devices generate, what is collected by servers and what persists on the device itself and thus could be extracted by those with the technical means. Unless we have the requisite skills, it is extremely difficult to gain insight, and mechanisms such as subject access requests, where data protection laws exist, are unlikely to give the full picture.

To illustrate this, we made a subject access request to Amazon in relation to an Echo Dot. We wanted to know what was stored on the device itself, as opposed to in Amazon's servers. Amazon stated:

> "Echo Dot devices store a limited amount of data locally. Although we have no obligation to provide you data that is held locally on your device and that we don't process, since you have specifically asked for it, we have extracted that data from your device…"
>
> "As mentioned, the amount of data that Echo Dot devices store locally is limited. Some data uses small caches that are constantly overwritten, such as our on-device technology for detecting the "wake word" and device logs."

If you are curious you can read more. on Amazon's answers.

Not only might there exist an information asymmetry between what the police can access compared to the victim, witness or accused, there is the additional issue that those investigating, or prosecuting will not have the requisite understanding as to the capabilities of connected devices.

Quality and reliability of evidence

Do the police know what they are doing?

Forensics is a complex area, particularly when we are taking about digital forensics[xvi] as we have highlighted in relation to mobile phone forensics.

Figure 3: Privacy International's response to the UK report on forensic science; highlighting police not understanding new tech, risk of incorrect inferences and lack of understanding about capabilities of forensic tools

At the investigative stage of legal proceedings an individual is likely to be at a significant disadvantage, because there will not have been any degree of disclose of evidence. If the

arrest is based on digital evidence then the information asymmetry between what the user can obtain from their device and what the police can obtain, is pronounced. The police are not only likely to have greater ability to obtain data from companies who collect the data generated by connected devices, they may have tools to extract data from devices directly.

Police are acquiring powerful tools to extract, decode and interpret the data from a wider array of connected devices. For example, the company Oxygen Forensic Detective markets products to exploit "Digital Assistants as the new eye-witness"[xvii]. They promise that:

> "Investigators, armed with Oxygen Forensic Cloud Extractor, can extract Amazon Alexa data to include these valuable recordings of that **actual utterance by the user**."
>
> "The valuable data can contain a wealth of information to include account and device details, contacts, user activity, incoming and outgoing messages, calendars, notifications, user created lists, created/installed skills, preferences, and more. One amazing feature in the software is the ability to extract the stored voice commands given to Alexa by the user. The *information extracted from Amazon will undoubtedly give tremendous insights into the user's everyday activity, their contacts, shared messages, and valuable voice commands*."
>
> "Oxygen Forensic Detective arms investigators with tools to *extract data from Google Home from both mobile devices and the associated cloud service*."

However, the heavy reliance on easy to use tools also brings new risks. Many believe it dumbs down digital forensics and creates significant risk of miscarriage of justice. Dr Jan Collie, Managing Director and Senior Forensic Investigator at Discovery Forensics told the UK House of Lords Science and Technology Committee that:

> "What I am seeing in the field is that regular police officers are trying to be digital forensic analysts because they are being given these rather whizzy magic tools that do everything, and a regular police officer, as good as he may be, is not a digital forensic analyst. They are pushing some buttons, getting some output, and quite frequently, it is being looked over by the officer in charge of the case, who has no more training in this, and probably less, than him. **They will jump to conclusions about what this means because they are being pressured to do so, and they do not have the resources or the training to be able to make the right inferences from those results. That is going smack in front of the court."**

Dr Gillian Tully, UK Forensic Science Regulator commented that:

> "There is a lot of digital evidence being analysed by the police at varying levels of quality."

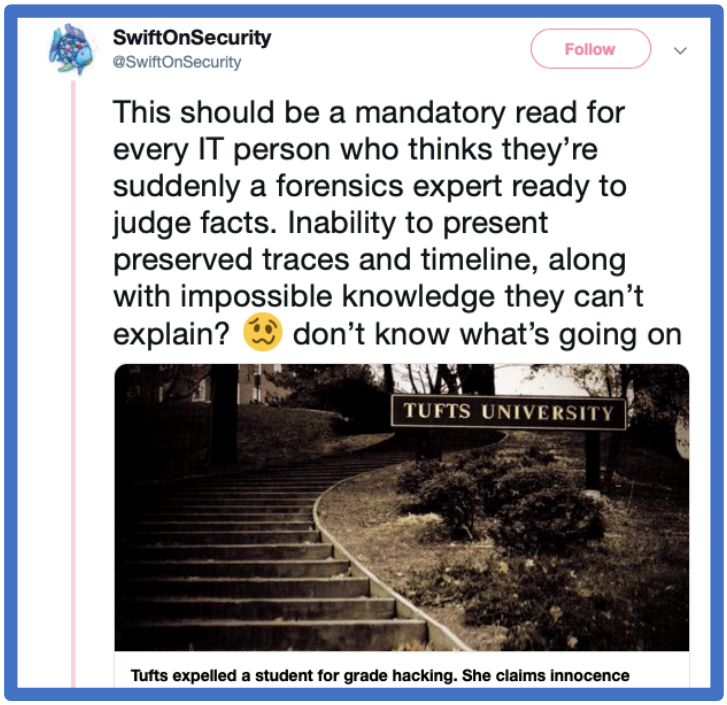
IoT forensics can be seen as a particular specialisation which portrays multiple challenges depending on the versatility and complexity of the IoT devices such as variance of devices, proprietary hardware and software; data present across multiple devices and platforms; proprietary jurisdictions for where data is stored.[xviii]

There has been little discussion about the risks of those without forensic expertise conducting digital forensics or drawing conclusions from the data they obtain. This is an issue not just in relation to complex devices such as mobile phones, but also in relation to a cheap connected device such as a WiFi enabled door bell. If push button technologies are to be used by those who have had limited or no training, then further informed debate is needed as to whether this should happen at all or what appropriate safeguards are needed.

One example of the risks relates to attribution. Attribution is hard and examining digital evidence requires expertise. In a recent case which highlights not only the risks associated with digital evidence but also information asymmetry, Tufts University expelled a student for grade hacking.[xix] The bulk of the evidence came from Tufts IT department, which said each incident as "well supported" from log files and database records. Commenting on the case and in particularly on the fact that the university held all the information, Samantha Harris, vice president of police research of at FIRE told Tech Crunch:

> "It's troubling when I read her appeal," said Harris. "It looks as though [the school has] a lot of information in their sole possession that she might try to use to prove her innocent, and she wasn't given access to that evidence."

@SwiftOnSecurity commented on the story:



The information asymmetry, created by data exploitation, risks enhancing inequality in defence causing insurmountable barriers for the accused to defend themselves.[xx]

The data storage of connected devices is mainly in the Cloud due to its scalability and accessibility. The National Institute of Standards and Technology, U.S. Department of Commerce, has a programme on Cloud Computing in Forensic Science aimed at contributing towards improved accuracy, reliability, scientific validity, and usefulness of cloud forensic

science. They state that one of the most daunting new challenges is how to perform digital forensics in the various types of cloud computing environments. For example, data collection challenges include locating forensic artefacts in large distributed and dynamic systems; locating and collecting volatile data and data collection from virtual machines.[xxi]

Another consideration is that the narrative built by the data collected by police is likely to be incomplete and may focus on part of a narrative that inculpates someone but overlook aspects that could exculpate them. Police investigators need to be trained to recognise the limitations of digital data and where necessary to use forensically sound methods to rely on this data. Without appropriate guidance and clear standards, police risk building criminal investigations on incomplete narratives and false conclusions, leading to miscarriages of justice. There is the added risk of assumptions made by juries on the basis of incomplete digital evidence, particularly when the defence is unable to determine whether such evidence is just one piece of a larger ocean of data.

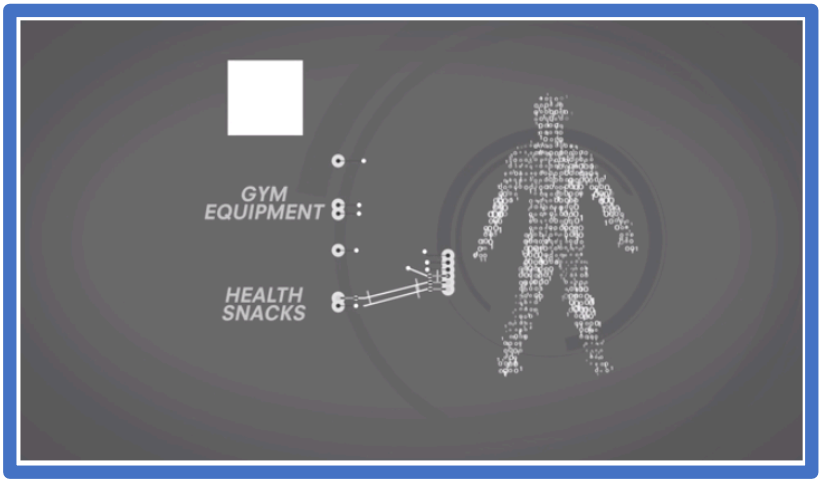
Are we allowed to know what the tech is doing?

Individuals do not have access to the same expensive technology as the police. Whilst they may be provided with the extracted data and perhaps an expert report of the prosecution, without forensic expert of their own, they are unlikely to have the ability to interrogate the forensic rigour of the extraction process. But even if they had the resources and sought to verify or challenge the conclusions of a digital forensics expert, as noted by the UK Parliament Science and Technology Committee, some private companies are unwilling to 'disclose information about their own development and testing methods [which] means that the evidence base for the correctness of many digital methods is extremely weak or non-existent.'

Device Insecurity: Unreliable evidence

Access controls, secure communication and secure storage are significant challenges in the IoT environment. As reported by Motherboard in 2015, "If you own a smart dildo **assume it's been hacked**"[xxii].

Data is generated and processed often on insecure and unstable technological foundations. For example, an LG Smart vacuum allowed a team of researchers to access live-stream video from inside the house[xxiii]. Devices were not designed with security in mind; instead, the main concern has been to minimise cost and size. Even devices we put inside our bodies are not sufficiently secured. The US Food and Drug Administration (FDA) had to recall pacemakers because they were deemed vulnerable to hacking[xxiv].



The quest for evidence from connected devices will go beyond well-known products such as the Amazon echo or Fitbits[xxv]. The irrationally exuberant desire to add connectivity to objects means a plethora of devices with creepy data-collection practices but also an ever-enlarging number of insecure devices that may be vulnerable to manipulation and distortion. **If we are to rely on connected devices in investigations or as evidence, questions need to be asked about the reliability of the 'evidence' they provide.**

> What are the implications, for evidential purposes, if your connected toaster has a microphone and a camera you did not know about, that can be accessed via a default admin password of 123, making it easy to interfere with or manipulate?

In order to ensure that connected devices are secure, safe, privacy respectful and reliable, they should be designed and built taking into consideration security and privacy risks from early on. If devices are insecure and can be accessed and manipulated, with little effort and minimal cost, there are implications for whether they can be trusted as a form of evidence. However, knowing that a device is insecure also requires technical expertise. So, whilst flaws in the security system might means the data has been compromised, this may not be immediately apparent.

The new UK "Code of Practice for consumer IoT security" constitutes a first attempt to guide all parties involved in the development, manufacturing and retail of consumer connected devices to ensure that products are secure by design[xxvi]. The Code, among others, sets out a series of practical guidelines for connected devices' manufacturers, recommending not to set default passwords, to have a vulnerability disclosure police, to update their software, ensure that personal data is protected, and to minimise exposed attack surfaces.[xxvii] Such initiatives are welcome, if limited in impact.

Looking at the issue from another angle, there is a further human element relating to the security and control of a device[xxviii]. Family members may be able to use devices, but they will not be aware that the controller of the device has access to every search, every move, every thought they make. In cases of domestic violence, police's awareness of who controls smart

and connected devices in the house might be proven crucial for the investigation and whether someone in the house manipulated the data.

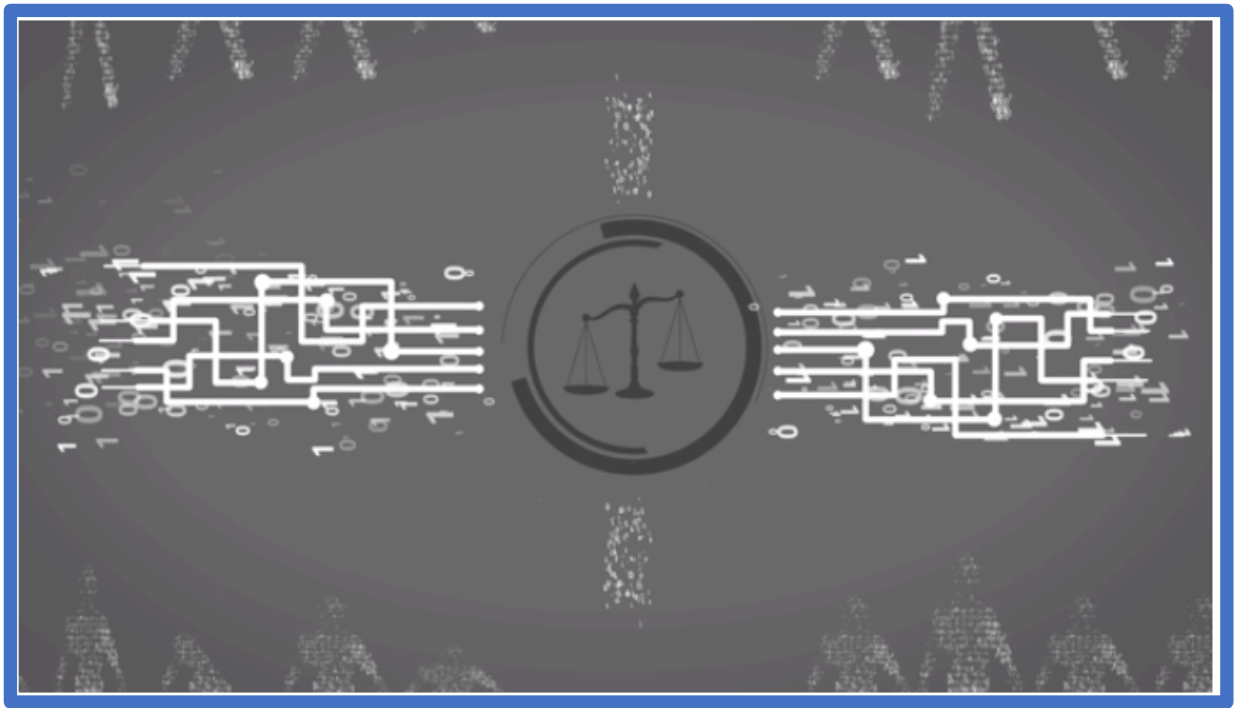
Access to justice

To be able to transform data to evidence, one needs expensive equipment to decode and analyse the data, as well as human expertise to interpret this data. When the poorest and most vulnerable in society are charged with serious offences, how are they to afford expensive expert evidence? They might be able to seek the raw data from their devices with the help of a lawyer, but that must be explained to the judge or to the jury, by an expert. If only the prosecution can present the evidence, how can the accused challenge, effectively, evidence they know to be incorrect or indeed evidence they don't realise is incorrect?

If there is digital evidence involved in a case, that needs to be obtained, interrogated and its significance understood. This requires expertise. The lack of probative challenge to the provenance and integrity of digital evidence from connected devices has the potential to result in erroneous convictions. Further, forensic science relies not only on accurate and reproducible detection and analysis of relevant materials, but also on evaluative interpretation of those materials in a specific context.

Experts may be needed not only to interpret the raw data, but also to address issues relating to the security of the devices, the potential for manipulation and general reliability of the evidence. Further, many devices not only generate data, but companies collect the data and use it to profile users and make inferences. What if this data also to be used either in investigations or as evidence?

In legal proceedings evidence must be interrogated effectively if we are going to remove a person's liberty, give them a criminal record or impose a fine. The principle of equality of arms and the right to an adversarial hearing are inherent components of the right to a fair trial. They require that each party has a reasonable opportunity to present their case under similar conditions. It includes the opportunity for the parties to have knowledge of and comment on all evidence adduced or observations filed with a view to influencing the court's decision. Any limitations should be strictly justified, and safeguards should be in place to protect the accused from the imbalance caused by these restrictions.[xxix]



Consider this issue in the context of a number of widely reported cases involving Fitbit data. A man was charged with murdering his wife in Connecticut based on evidence from the victim's Fitbit data[xxx] and in another case Fitbit data has been used to investigate whether a 90-year old murdered his stepdaughter[xxxi]. In the former case, the accused told police that a masked assailant "with a Vin Diesel voice" came into the couple's suburban home at around 9am on 23 December 2015. He subdued the husband using "pressure points" before shooting his wife as she returned through the garage. However, the victim's fitness tracker told a different story. According to data from the device, which uses a digital pedometer to track the wearer's steps, the victim was moving around the house for more than an hour after her husband said the murder took place. In January 2019 it was reported that Richard Dabate 'rejected a plea deal offer' and wants to 'take the case to trial'[xxxii]. The role of digital evidence in the trial itself is to be seen. But even in cases that appear to be open and shut, we should not forget that digital forensics is complex.

The ability to access expert evidence, even if the case is going to trial, is not guaranteed and will depend on the jurisdiction and whether individuals can access, for example, legal aid. As with other types of forensics, if this is to be used against you, there are implications for equality of arms if the prosecution can rely upon expertise that is not available to the individual.

In order to be useful in court digital evidence often requires interpretation by experts. A well-known case where prosecutors relied upon a digital witness involves a pacemaker – a connected device inside the individual's body. A man from Middletown, Ohio, was indicted in January 2018 for aggravated arson and insurance fraud for allegedly setting fire to his home in September 2016. The Ohio authorities obtained and looked the data recorded on the pacemaker. In order to be admissible as evidence in court, an expert statement by a cardiologist was necessary. There are additional issues around chain of custody witnesses.

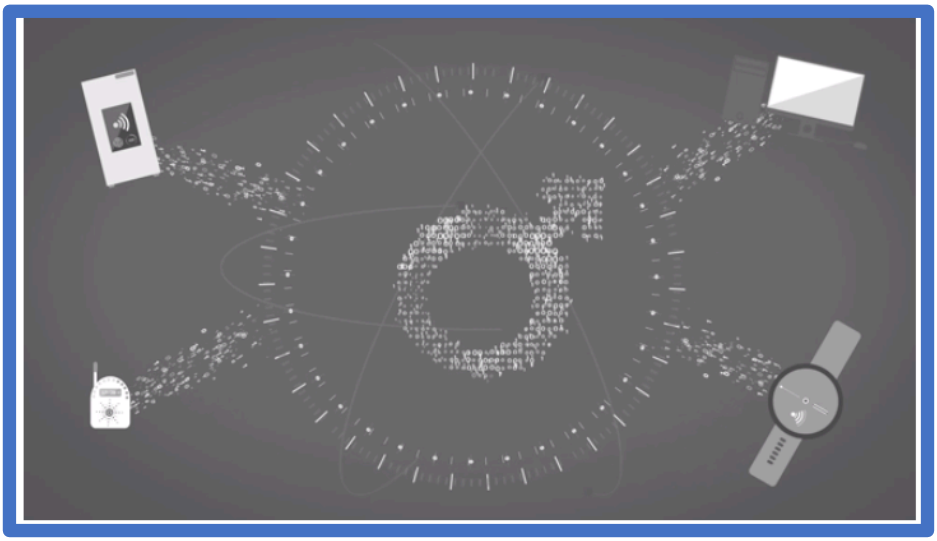
A recent report by the UK Parliament Science and Technology Committee noted that in many criminal cases forensic science evidence is pivotal, and the delivery of justice depends on the integrity and accuracy of that evidence. **Despite the rapid growth in digital forensic evidence there is no discernable strategy to deal with the challenge this presents to the criminal justice system.** The report went on to warn that fair access to justice for defendants is hampered by cuts to legal aid[xxxiii]. 'The defence must have the opportunity to commission their own forensic testing where evidence is disputed.'

There is a discrepancy between what the police, prosecution and a privately funded client can commission compared to an individual with no money. It is not the case in every jurisdiction that individuals have the right to state funded expert. And even if they did, if there are funding constraints, that may impact on the type and quality of expert they can obtain, compared to the State.

The state will have access to resources to prosecute individuals that are not at the disposal of those individuals to challenge the state's evidence or to exculpate themselves. The lack of access to appropriate tools and expertise on behalf of individuals risks creating new forms of inequalities in the criminal justice system, governments must review where appropriate that legal frameworks and procedures are in place.

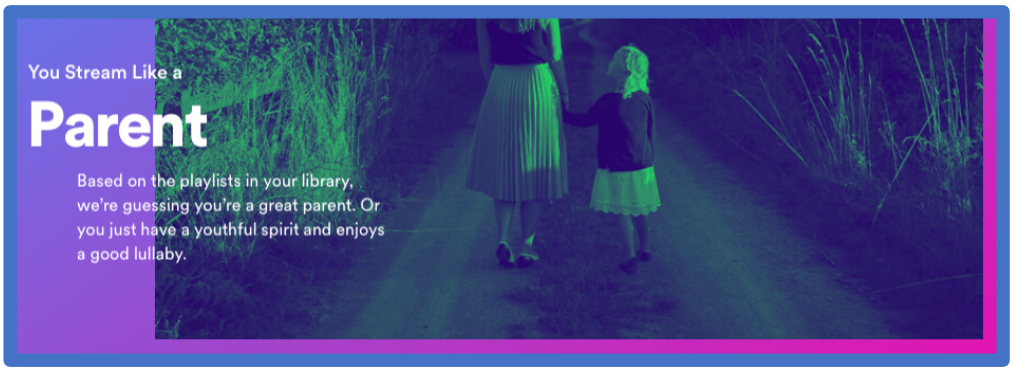
Automated analysis and profiling

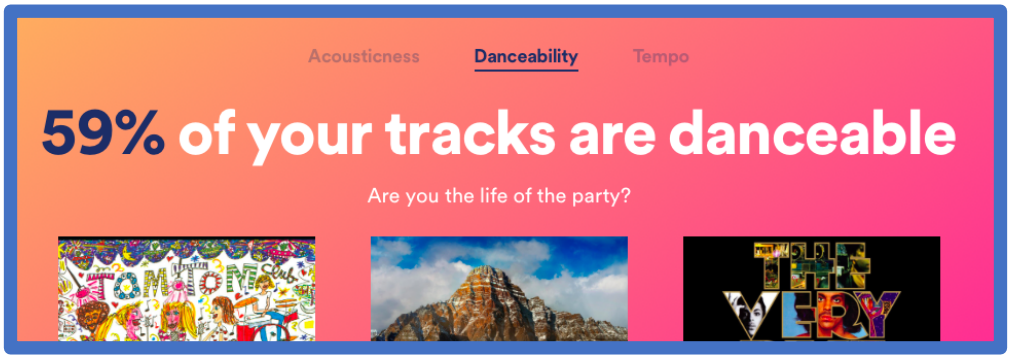
Data is increasingly interpreted through automated analysis, for instance profiling, adding a layer of complexity. Companies and governments rely less on data we provide and instead look at data they can observe, derive, and infer. Add into the above the spectre of machine learning and the loss of control goes even further. Data can tell a lot about a person, but through profiling and machine learning, one can learn patterns, make predictions and inferences that we usually don't have access to. Let alone are able to interrogate for purposes of veracity. Whether stored on the device or in Cloud storage, the police may be able to access this information[xxxiv].



Whether it is Experian or Spotify, they have profiled you based on the data accessible to them. What does this mean for your defence if those profiles are used as evidence against you?

A quick example of profiling is Spotify's Spotify.me. According to Spotify:





Whether these forms of profiling would ever be used as evidence is questionable. But as more data is gathered, more profiling carried out, what inferences based upon user behaviour may be sought to impugn someone's character?

Conclusions

We are constantly buying new things that have the ability to connect and transmit data to our phone, to the Cloud, to each other. As digital "informants" around us proliferate, the digital data they produce will ever increase. According to what is considered a conservative calculation, there will be approximately 25 billion devices by 2020[xxxv].

The police seek data from the devices that surround us, companies develop the tools to enable easy extraction and we continue to buy these products with little thought about how they could betray us and cause future miscarriages of justice. The reporting on crimes where connected devices form part of the evidence can often present this new frontier as offering the silver bullet to complex criminal investigations. We need to step back, take a broad view on the risks and challenges and seek basic guarantees for the crime scene of the future.

As the technology and law stand, it seems that we are not ready for the future that is already being built and our laws are not yet able to address the risks that are posed.

[i] Currently described as the Internet of Things (IOT).

[ii] https://www.dickinson-wright.com/news-alerts/legal-and-privacy-issues-with-connected-toys
[iii] https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html
[iv] Ms Smith, "Nest Secure Had a Secret Microphone, Can Now Be a Google Assistant." CSO Online, 5 February 2018, available at https://www.csoonline.com/article/3336227/nest-secure-had-a-secret-microphone-can-now-be-a-google-assistant.html.
[v] Darlene Storm, "NSA Interested in Exploiting Internet-Connected Medical Devices, Spying on IoT", *Computerworld*, 13 June 2016, available at https://www.computerworld.com/article/3082162/nsa-interested-in-exploiting-internet-connected-medical-devices-spying-on-iot.html
[vi] Detectives are being trained to identify digital footprints and with so much data at the tip of their fingers, the UK police plan to develop a digital forensics kit which would allow investigators to download data from the crime scene and screen data from microchips.
[vii] India Ashok, "Smart devices may soon provide UK police with evidence of crime – report", International Business Times, 2 January 2017, available at https://www.computerworld.com/article/3082162/nsa-interested-in-exploiting-internet-connected-medical-devices-spying-on-iot.html
[viii] Alina Selyukh, "As We Leave More Digital Tracks, Amazon Echo Factors In Murder Investigation", npr, 28 December 2016, available at https://www.npr.org/sections/alltechconsidered/2016/12/28/507230487/as-we-leave-more-digital-tracks-amazon-echo-factors-in-murder-investigation
[ix] Meagan Flynn, "Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over", *Washington Post*, 14 November 2018, available at https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/
[x]https://www.huffingtonpost.co.uk/entry/amazon-arkansas-murder-case_n_58642d86e4b0eb586488082c?guccounter=1&guce_referrer=aHR0cHM6Ly9jb25zZW50LnlhaG9vLmNvbS8&guce_referrer_sig=AQAAAJaJ96aR-2p4Y9KDcvNCA8sn3tfCBSpCegMhIyiJpU6Q1EhJ4dSxXhiXGVcTzqOGQAs_BBjwS_AglN53nKiWwRtJPL4EeHzAFmYubs5V6x4LruDQuRvlsOqRwxOFuwU-c1QXDcgE-B35UOhaMZybQWSkHrWj0Anewvx5ohVxbYw6

[xi] https://www.hja.net/why-you-should-be-concerned-by-amazon-potentially-hiding-alexa-in-your-internet-router-the-admissibility-in-court-for-the-evidence-retrieved/

[xii] Privacy International: "Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad", 8 November 2018, available at http://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad. See also on data manipulation Privacy International, Report: "How Apps on Android Share Data with Facebook," 29 December 2018, available at http://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report.
[xiii] Philips: Frequently Asked Questions: Why Does My Philips Sonicare App Requires Permissions, available at https://www.usa.philips.com/c-f/XC000015330/why-does-my-philips-sonicare-app-requires-permissions.
[xiv] "Moz://A *privacy Not Included - Eight Sleep Mattress", https://foundation.mozilla.org/en/privacynotincluded/products/eight-sleep-mattress/.
[xv] Joseph Cox, "A Sex Toy Lawsuit Highlights Privacy Concerns Around 'Smart' Dildos." Motherboard (blog), 14 September 2016, available at https://motherboard.vice.com/en_us/article/bmv5ja/a-sex-toy-lawsuit-highlights-privacy-concerns-around-smart-dildos.
[xvi] Zack Whittaker, "Tufts Expelled a Student for Grade Hacking. She Claims Innocence", *TechCrunch*, 18 April 2019, available at http://social.techcrunch.com/2019/03/08/tufts-grade-hacking/.
[xvii] Oxygen Forensic Detective: Digital Assistants as the New Eye-Witnesses, available at https://www.oxygen-forensic.com/en/uploads/doc_guide/IoT_web.pdf.

[xviii] Boricha, V, "IOT Forensics: security in an always connected world where things talk" (May 2018) available at: https://hub.packtpub.com/iot-forensics-security-connected-world/
[xix] Zack Whittaker, "Tufts Expelled a Student for Grade Hacking. She Claims Innocence", *TechCrunch*, 18 April 2019, available at http://social.techcrunch.com/2019/03/08/tufts-grade-hacking/.
[xx] @SwiftOnSecurity, see https://twitter.com/SwiftOnSecurity/status/1104189457069236224.
[xxi] NIST Cloud Computing Forensic Science Challenges, (June 2014) Available at: https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf
[xxii] Nicole Kobie, "Yes, Your Smart Dildo Can Be Hacked", *Motherboard*, 10 February 2015, available at https://motherboard.vice.com/en_us/article/ae3y8e/yes-your-smart-dildo-can-be-hacked.
[xxiii] Ben Popken, Hacked Home Devices Can Spy on You, NBC News, 26 October 2017, available at https://www.nbcnews.com/tech/security/hacked-home-devices-can-spy-you-n814671
[xxiv] Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication, 29 August 2017, available at https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm.
[xxv] Harriet Alexander, "Man Charged with Wife's Murder after Her FitBit Contradicts His Timeline of Events", *The Telegraph*, 25 April 2017, available at https://www.telegraph.co.uk/news/2017/04/25/man-charged-wifes-murder-fitbit-contradicts-timeline-events/.
[xxvi] Code of Practice for consumer IoT security, Secure by design, Department for Digital, Culture, Media & Sport, UK Government (2018), available at Code of Practice for consumer IoT security, Guidelines, Department for Digital, Culture, Media & Sport, UK Government (2018), available at https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.
[xxvii] Code of Practice for consumer IoT security, Guidelines, Department for Digital, Culture, Media & Sport, UK Government (2018), available at https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.
[xxviii] Leoni Tanczer ao, "Gender and IoT Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse", UCL in collaboration with PETRAS, London VAWG Consortium and Privacy International, London, November 2018, available at https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf. See also Rachel Cericola and Kaitlyn Wells, "How to Keep Your Smart-Home Technology Secure From Domestic Abusers", *Wirecutter*, 23 October 2018, available at https://thewirecutter.com/blog/keep-your-smart-home-secure-from-domestic-abusers/; Tom Harper and Nicholas Hellen, "Smart Gadgets Open Door to Stalking and Abuse, Say Police", *The Sunday Times*, 13 January 2019, available at https://www.thetimes.co.uk/article/smart-gadgets-open-door-to-stalking-and-abuse-say-police-5xk8n7r9m.
[xxix] Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb), European Court of Human Rights, Council of Europe, Updated on 31 December 2018.
[xxx] Tracy Connor, "Fitbit Murder Case: Richard Dabate Pleads Not Guilty in Wife's Death", *NBC News*, 28 April 2017, available at https://www.nbcnews.com/news/us-news/fitbit-murder-case-richard-dabate-pleads-not-guilty-wife-s-n752526.
[xxxi] "Fitbit Data Used to Charge Man with Murder," BBC News, 4 October 2018, available at https://www.bbc.com/news/technology-45745366.
[xxxii] https://www.apnews.com/b7461ed3e0294fc79a12bebd15af2b69

[xxxiii] If you can't afford legal advice or support in court, you might be able to get free or cheaper help. https://www.citizensadvice.org.uk/law-and-courts/legal-system/finding-free-or-affordable-legal-help/
[xxxiv] Privacy International, "Digital Stop and Search: How the UK Police Can Secretly Download Everything from Your Mobile Phone," 27 March 2018, available at http://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-

download-everything-your-mobile. See also, Privacy International: Phone Data Extraction, available at https://privacyinternational.org/campaigns/phone-data-extraction.

[xxxv] Colin Barker, "25 Billion Connected Devices by 2020 to Build the Internet of Things", *ZDNet*, 11 November 2014, available at https://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/.