Burkhard Schafer:

D-waste: Data disposal as challenge for waste management in the Internet of Things

Abstract:

Proliferation of data processing and data storage devices in the Internet of Things poses significant privacy risks. At the same time, faster and faster use-cycles and obsolescence of devices with electronic components causes environmental problems. Some of the solutions to the environmental challenges of e-waste include mandatory recycling schemes as well as informal second hand markets. However, the data security and privacy implications of these green policies are as yet badly understood. This paper argues that based on the experience with second hand markets in desktop computers, it is very likely that data that was legitimately collected under the household exception of the Data Protection Directive will "leak" into public spheres. Operators of large recycling schemes may find themselves inadvertently and unknowingly to be data controller for the purpose of Data Protection law, private resale of electronic devices can expose the prior owner to significant privacy risks.

Agenda:

Author:

Prof. Burkhard Schafer:

- University of Edinburgh, SCRIPT Centre, School of Law
- ☎ + 44 - 131 - 65 02 03 5 , ✉ b.schafer@ed.ac.uk, 💻 http://www.law.ed.ac.uk/people/burkhardschafer
- Relevant publications:
  - with Judith Rauhofer, Zbigniew Kwecka, William Buchanan, '"I am Spartacus" : privacy enhancing technologies, collaborative obfuscation and privacy as a public good' (2014) Artificial Intelligence and Law vol 22 p113-139.
  - with Wiebke Abel 'Guter Ork, Böser Ork: Snowden und die staatliche Überwachung von Online-Spielen in Grossbritannien' (2014) Jusletter-IT Vol 6 RZ 1-43 Vl 6.

ISSN 1614-1687

In the digital world, preventing others from acquiring information about us is just as difficult as to rid ourselves of data that we do not needed any longer. There might now be a recognised right to be forgotten, but our ability to "forget", especially for ordinary users of technology without specialist training, could turn out to be more limited than anticipated. Experts in computer forensics know just how difficult it is to delete information so that it cannot be reconstructed and retrieved again.[1] This raises particular challenges for the Internet of Things – when I resell my car or my fridge, or when I bring my washing machine to a recycling point, can I make sure that I do not leave data on them behind that could potentially tell others more about me than I am comfortable with?

Environmental vs Data Protection: setting out the conflict

With the proliferation of sensors, communication and data storage devises in the Internet of Things, concerns about privacy have increasingly come to the fore. In this new world, your car knows potentially more about you than your parents or partner - where exactly you travelled to last night, for instance, and maybe even if you were alone or the second seat was adjusted by someone.[2] In this future your fridge potentially talks to your toilet about providing a healthier diet for you, resulting in sensitive personal data that is collected, stored and exchanged in unprecedented quantities.[3] The debate on privacy in this interconnected world has created a lively academic debate.[4] In these discussions, the focus however is exclusively on the acquisition, use and storage of data while the equipment is in actual use and fully functional. This is not an unreasonable focus. After all, it is at this stage that very often a third party will be involved. To "know" where it is, my car has to communicate with an internet based service that provides this information, and the medical toilet will typically come as part of an integrated care home solution that also communicates with a care home provider or medical professional. The danger for the user of these devises then is abuse of this data by third parties, either through actions by that service provider directly (e.g. by reselling personal information) or through actions of others, be it criminals who succeed in compromising the security of my service provider, or by law enforcement agencies that acquire the data legally as part of an investigative process. Data acquisition and storage during the working life of an intelligent device undoubtedly covers the most important part of the life-cycle of electronic equipment, but nonetheless not all of it. Less prominent in the public awareness, and much less intensively discussed, is the destiny of the data once a device has reached the end of its working life, or at least the end of its usefulness for the current owner.

This aspect of secure data storage and disposal interacts in problematic ways with other societal costs of ubiquitous digital devices. While we often treat communication technology as mere abstract flow of data, we must not lose sight of the physical substratum that enables the exchange of data, the hardware that we use and more importantly, discard in ever-shorter cycles of consumption.[5] The global environmental problems that are created when the technology available to safely dispose of discarded equipment is outpaced by technological innovation of the gadgets themselves were recently the topic of a special issue of the International Review of Information Ethics[6]. Electronic waste or e-waste is increasingly recognised as an environmental problem in

[1] See for an example Thing and Tan 2012

[2] On privacy and autonomous vehicles in general see e.g. Glancy 2012

[3] See for one vision of this specific smart device Schlebusch et al. 2014

[4] See for an overview of the debate e.g. Weber, 2010; Medaglia and Serbanati 2010.

[5] See for an empirical study e.g. Environmental Protection Agency (EPA) 2008

[6] See Feilhauer et al. 2009

developed and developing countries,[7] with the latter often the recipient of waste from the former.[8] One important strategy to minimise the problem of e-waste is to prolong the consumption life cycle of electronic goods.

Following Lessig's concept of four distinct modes of regulation for the information society, we can distinguish between legal, market based and technological approaches to this problem. Prominent regulatory approaches are mandatory take-back and/or recycling schemes. From the 1990s onward, the "end of life challenge" – how can we safely dispose the ever increasing numbers of obsolete electronic products that contained significant quantities of hazardous materials - led the European Union to adopt the principle of "Extended Producer Responsibility" (EPR).[9] EPR makes manufacturers responsible for the full costs of their products across their lifecycle, thus internalising costs that are otherwise negative externalities. A typical way to achieve this are take-back obligations for their products once they reach the end of their useful lives. This can be combined with mandatory recycling schemes and targets for recycling.[10] Regulatory schemes like these create incentives for manufacturers to build equipment in a way that it reduces the costs of recycling, and/or by extending the life cycle of their products by design. Regulation by design is the second mode of regulation in Lessig's scheme. Finally, there are purely market based solutions. A flourishing second hand market in particular can extend the life cycle of goods that are abandoned by their owners not so much because they stop working properly, but because of social pressure, considerations of status and fashion.[11]

Reverse-logistics and mandatory take-back are at the heart of the Waste Electronic and Electrical Equipment (WEEE) directive (Directive 2002/96/EC) that established in Europe Extended Producer Responsibility.[12] While particularly rigorous in its demands, other countries are now slowly adopting similar approaches to the regulation of e-waste, though often with significant delays.[13]

At first sight, things look good, at least in Europe. We have an increasingly mature discussion about privacy concerns with regards to the Internet of Things. The upcoming Data Protection Regulation will enshrine the concept of Privacy by Design into law and substantially sharpen the responsibilities of data controllers. This will in particular also ensure better data protection in ubiquitous computing environments and the Internet of Things, where users will often be unaware of the fact that their personal data is gathered by their environment.[14] At the same time, we have a rigorous debate about the environmental impact of the hardware aspects of the IoT, in particular when it comes to e-waste. However, so far these two debates have not been linked with each other, and as we argue, this should be a cause for concern. If we increasingly resell, recycle or repurpose electronic devices, and if these devices increasingly store personal data about us, then the question arises how this data in turn can be safely disposed of. The aim of the WEEEE directive is to reduce hazardous waste, but "hazardous" is understood in terms of physically harmful substances only, the lead, cadmium or mercury that they contain, not the abstract and intangible information that they carry. Depending on the nature of the device, this information however can be potentially hazardous too, and in particular expose the previous

[7] Babu, Anand, and Basha. 2007

[8] See e.g. Wong, et al. 2007

[9] Smith, 2009 p 9

[10] Recycling targets need not be linked to EPR of course. It is also possible to require municipal authorities to organise and run recycling facilities. If these in turn are paid for by manufacturers proportionally to use, the same effects as EPR should ensue. "Free standing" mandatory recycling schemes where public entities rather than the manufacturer is legally and financially responsible have different effect on product design and manufacturer behaviour, but for our purpose, data security and privacy, pose the same issues

[11] See e.g. Geyer and Blass V 2009 or Skerlos, et al 2003. Though under some conditions, second hand markets can also increase the demand for new goods, by reducing the costs of an upgrade. See e.g. Thomas, 2003.

[12] Sachs,. 2006

[13] Ongondo, Williams, and Cherrett. 2011

[14] Kiss and Szőke 2015

owner to risks. Not only are the two debates not linked, at least in part, they are pursuing opposite goals. From a data protection perspective, the safest way, and for many technologically unsophisticated users the only feasible one, is not to resell their gadgets or give them to a recycle centre for refurbishing or other forms of reuse, but to put a hammer to the storage device and physically destroy it.[15] This can be in itself causing an environmental harm and it most certainly prevents extending the product's life cycle though reuse or resale. By contrast, resale or refurbishment are most likely to be successful if as much of the computational capability of the product is preserved, functional software should potentially be left on the device and only personal data should be deleted.

The conflict between the two objectives comes into even starker relief when we look at digital object memories, software objects intentionally designed to record the "life experience" of an object. Research has shown that such digital memories can increase the resale value of second hand electronic goods. Research in the Tales of Things and Electronic Memory (TOTeM) project approached the Internet of Things from this very perspective. It notes that our habit to surround ourselves with mementoes, objects with very strong personal resonance, faced in the past the problem that passage of time or change of ownership can mean that the stories behind this emotional meaning can get lost to future generations.[16] With digital memories associated with these objects, this danger decreases.[17] This has obvious implications for the second hand market, especially collectors. For obvious reasons, if I plan to sell the silver knife that was passed on through generations in my family, being able to demonstrate that it was given to my ancestor by Wellington at the Battle of Waterloo as a replacement for the dagger he threw to protect the general's life will increase its value immeasurably. Pierce and Paulos were amongst the first to identify the potential of digital memories for what they call "reacquisition and dispossession",[18] the sale and acquisition of second hand goods in charity shops or antique fairs. They proposed to enhance reacquisition practices explicitly with a focus on sustainable consumption, suggesting to digitally record the "histories of possession, maintenance and repair" of everyday objects. The TOTeM project developed these ideas further, showing how digital memories can enhance resale value.[19]

Quantifying the problem

We now have developed the broad setting for our discussion: from the perspective of environmental protection, we should increase resale, refurbishment, reuse and repurposing of electronic devices, including internet enabled devices in the IoT. For this, they need to reserve as much of other functionality has possible, and may even benefit from "added" information that tracks their history. From a Data Protection perspective, data minimisation and secure storage requirements should make us hesitant to give possession of any of these devices to third parties, even at their end of (for us) useful life. As noted above, there is at the moment a dearth of empirical studies on "information leakage" from second hand IoT devices. However, the related problem of security risks created by second-hand PCs has received attention for some time now.

[15] Physical destruction of hard drives is often recommended for particularly sensitive information when disposing of compute equipment. See e.g. http://abouthipaa.com/wp-content/uploads/NIST-Special-Publication-800-88_Guidelines-for-Media-Sanitization_SP800-88_rev1.pdf. The methods mentioned there are all environmentally hazardous and require specialist skills.

[16] Barthel, et al. 2013

[17] Bell and Gemmell, 2009

[18] Pierce, and Paulos. 2011

[19] de Jode, et al. 2012.

Even with traditional computers, privacy conscious recycling is a concern. The problem of data remanence in "automated information systems" was identified first by the US military in the 1960s.[20] In the 1980s, the National Security Agency became responsible for computer security within the Department of Defense and commissioned a series of studies at the Illinois Institute of Technology, and Carnegie-Mellon University to evaluate the efficiency of secure data sanitization such as degaussing, physical destruction and various forms of overwriting. While the security culture of the military and the technical infrastructure available to them thus ensured that their computers were safely prepared for reuse, neither their level of awareness, nor their technical abilities, found a counterpart in the civilian sector. There, anecdotal stories of inadvertent data disclosure through reselling, donating or otherwise discarding of personal and company computer abound. In 1997, a resident of Nevada bought a used IBM computer and discovered that it contained the prescription records of 2,000 patients, including their names, addresses and Social Security numbers, a list of the medication they had been prescribed (some for alcoholism and depression). The computer could be traced back to a pharmacy that had sold it when updating their computer system. In 2001, a US company auctioned off more than 100 computers which confidential client information. In 2002, a United States Veterans Administration Medical Center in Indianapolis discarded over 100 computers, donating some to schools while selling others. Some ended up in second hand shops where a journalist bought one, only to find that the computer contained highly sensitive medical information, including the names of veterans with AIDS and mental health issues. In addition to the medical data, credit card information was also stored on the device and easily recoverable.[21] Subsequent systematic studies confirmed again and again this picture. Back in 2000, Garfinkel and Shelat bought 158 hard drives on the secondary from a variety of sources, specialist second hand computer retailers to small companies selling directly their own surplus equipment. Many of the purchases were done through ebay. Even from this small sample, they were able to retrieve thousands of credit card details, significant amounts of personal and business emails and letters and also medical data.[22]

While Garfinkel and Shelat thought in 2003 that wider awareness of privacy risks in second hand computer markets would quickly reduce this problem, subsequent studies very consistently find the same problem reoccurring, independent of the details of the data storage technology, the sector (medical service providers continue to figure prominently event though privacy awareness in general has risen dramatically in that profession), country or age group.[23]

On the basis of this research, we can make an *a fortiori* argument: Data stored on personal computers is highly conspicuous – we know it is there because in most cases, we had to add it directly and explicitly. Personal computers are easily identifiable through their visual design. Slightly more difficult, but still relatively easy, is to identify their data storage component. Furthermore, physical removal of the hard drive is in many cases unnecessary, as user-friendly tools such as CCcleaner and other anti-forensic software allow secure data overwrite even to unsophisticated users. Despite this relative ease to prepare a personal computer for resale in a privacy preserving way, we find again and again that individual users, but also larger organisations, fail to take the necessary steps. In the IoT, none of these advantages are present: Data will often be collected without explicit user input, the diversity of smart devices makes it impossible to say just from visual inspection if an object is storing or processing data, and if so which type of data (one can think e.g. of smart clothing and jewellery). The precise space where data is stored will often be difficult to access (e.g. in a fridge or a central heating system) and they will not normally run software that allows easy data deletion.

[20] National Computer Security Center, "A Guide to Under- standing Dataremanence in Automated Information Sys- tems," Library No. 5-236,082, 1991 http://fas.org/irp/nsa/rainbow/tg025-2.htm

[21] all three cited in Garfinkel, and Shelat 2003 p.17-18

[22] ibid p. 24-26

[23] see e.g. El Emam, Neri, and Jonker 2007; Jones, Valli, and Dabibi. 2010;.Szewczyk. 2011; Lim et al 2014

Mitigation Strategies

What can we do to reduce the inherent risk for data security that recycling smart electronic goods in the IoT brings, while maintaining the benefits of mandatory take-back schemes and strong second hand market in electronic goods?

First, there are legal issues to consider. On the one hand, discarded data has to be recognised as an issue for the purpose of data protection law, while at the same time we must be careful not to overburden recycling providers or small second-hand retailers. In some jurisdictions, data discarded by its owner loses all legal protection. In the US, *California v. Greenwood* ensures that data on discarded devices do not enjoy a reasonable expectation of privacy. The discussion above should have made it clear how problematic this precedent is when applied to smart devices in the IoT. In addition, it also highlights a problem that European based recycling companies will face if they aim to transport the discarded good to other countries for refurbishment – inadvertently they may in the process transfer personal data outside the protection of EU law. In Europe, the legal situation is not quite as dire. Especially when customers are de facto forced to use a recycling service as the only lawful means (under environmental law) to discard used electronic equipment, the resulting power imbalance will be recognised by the new Data Protection Regulation. This means in particular that discarding a device in this way will not be constructed as implied (or possibly even explicit) consent to allow unfettered use of that data by third parties. Conversely, EU data protection law in interaction with the WEEE Directive also offers some protection for the organiser of recycling schemes: While they become data processors, or possibly in some set-ups even data controllers, the WEEE Directive provides a legal ground for the processing of the data. However, this privileges possibly unduly recycling operators set up to fulfil EPR duties of manufacturers over those who organise recycling schemes out of altruistic environmental or social concerns. Accessing data for the sole purpose to delete it as part of a recycling or resale/refurbishment scheme should therefore always be considered as a "legitimate interest".

This still creates burdens on operators of recycling schemes or second hand retailers, and also leaves risks for users. This burden can be minimised to a degree through design choices – ideally, the data storage component should be easily accessible, the data storage unit easily removable, and user data and other software stored separately. This should prevent the need to destroy equipment just to erase personal data, as discussed above. Easy ways to effect a "factory reset" that deletes all user data, while not as secure as using scrubbing software, would be highly desirable. "Privacy by design" is likely to be explicitly mentioned in the new Data Protection Regulation. Here Data protection law can learn from environmental law and ensure that "privacy by design" covers not just the operation of a device, but also the "D-waste" at the end of the lifecycle of a device. In the long run, the problems outlines above may require rethinking the "household exception" of Data Protection law. Given the complexity of compliance with DP law, it is on the one hand very reasonable to exempt data that is collected and processed in a purely domestic setting, e.g. my address list on my mobile phone. Much of the data in smart devices will be of that nature. But as our discussion shows, sound environmental principles make it inevitable that few devices will stay forever within the confines of just one household. That often the data is the data of the owner of a device only, or data of others collected lawfully under the household exemption, should not mean that we cannot think of reasonable safeguards when the data is discarded. A mandatory labelling scheme for smart devices that uses a traffic light warning system could for instance help the owner of a device to carry out an informal privacy risk assessment (make informed choices) when preparing a device for private resale or for return to a recycling scheme.

References

Dong, Tao. "Design Consideration of a Health-Information-Technology-Supported Intelligent Urinalysis System." In Advanced Materials Research, vol. 989, pp. 1077-1081. 2014.

Thing, Vrizlynn LL, and Darell JJ Tan. "Symbian smartphone forensics and security: Recovery of privacy-protected deleted data." Information and Communications Security. Springer Berlin Heidelberg, 2012. 240-251

Feilhauer, Matthias, et al. "Ethics of waste in the information society." special issue of International Review of Information Ethics 11 (2009)

Glancy, Dorothy J. "Privacy in Autonomous Vehicles." Santa Clara L. Rev. 52 (2012): 1171

Schlebusch, Thomas, et al. "Unobtrusive and comprehensive health screening using an intelligent toilet system." Biomedical Engineering/Biomedizinische Technik (2014). DOI: 10.1515/bmt-2013-0140, October 2014

Weber, Rolf H. "Internet of Things–New security and privacy challenges." Computer Law & Security Review 26.1 (2010): 23-30

Medaglia, Carlo Maria, and Alexandru Serbanati. "An overview of privacy and security issues in the internet of things." In The Internet of Things, pp. 389-395. Springer New York, 2010

Wong, M. H., et al. "Export of toxic chemicals–a review of the case of uncontrolled electronic-waste recycling." Environmental Pollution 149.2 (2007): 131-140

Babu, Balakrishnan Ramesh, Anand Kuber Parande, and Chiya Ahmed Basha. "Electrical and electronic waste: a global environmental problem." Waste Management & Research 25.4 (2007): 307-318

Thomas, Valerie M. "Demand and Dematerialization Impacts of Second-Hand Markets." Journal of Industrial Ecology 7.2 (2003): 65-78

Geyer R, Doctori Blass V (2009) The economics of cell phone reuse and recycling. Int J Adv Manuf Technol 47(5-8):515- 520

Skerlos SJ, Morrow WR, Chan KY, Zhao F, Hula A, Seliger G, Basdere B, Prasitnarit A (2003) Economic and Environmental Characteristics of Global Cellular Telephone Remanufacturing. In: IEEE InternationalSymposiumon Electronics and the Environment, 2003, 99–104. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1208055

Sachs, Noah. "Planning the funeral at the birth: Extended producer responsibility in the European Union and the United States." Harv. Envtl. L. Rev. 30 (2006): 51

Ongondo, Francis O., Ian D. Williams, and Tom J. Cherrett. "How are WEEE doing? A global review of the management of electrical and electronic wastes." Waste management 31.4 (2011): 714-730

Kiss, Attila, and Gergely László Szőke. "Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation." Reforming European Data Protection Law. Springer Netherlands, 2015. 311-331

Barthel, Ralph, et al. "An internet of old things as an augmented memory system." Personal and ubiquitous computing 17.2 (2013): 321-333

Pierce, James, and Eric Paulos. "Second-hand interactions: investigating reacquisition and dispossession practices around domestic objects." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2011

de Jode, Martin, et al. "Enhancing the'second-hand'retail experience with digital object memories." Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, 2012

Smith, Ted. "Why we are „Challenging the Chip ‟: The Challenges of Sustainability in Electronics." International Revie of Information Ethics11 (2009): 9.

Garfinkel, Simson L., and Abhi Shelat. "Remembrance of data passed: A study of disk sanitization practices." IEEE Security & Privacy 1.1 (2003): 17-27.

El Emam, Khaled, Emilio Neri, and Elizabeth Jonker. "An evaluation of personal health information remnants in second-hand personal computer disk drives." Journal of medical Internet research 9.3 (2007)

Szewczyk, Patryk. "Analysis of Data Remaining on Second Hand ADSL Routers." Journal of Digital Forensics, Security and Law 6.3 (2011): 17-30.

Jones, Andy, Craig Valli, and G. Dabibi. "The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market." 7 th Australian Digital Forensics Conference. 2009.

Lim, Charles, Ivan Firdausi, and Andry Bresnev. "Forensics Analysis of Corporate and Personal Information Remaining on Hard Disk Drives Sold on the Secondhand Market in Indonesia." Advanced Science Letters 20.2 (2014): 522-525.