Legal Information Management, 13 (2013), pp. 119–123

doi:10.1017/S1472669613000285

Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime

Abstract: This article aims to identify and define some of the legal issues, the computer misuses and the information misbehaviour associated with IT security that are increasingly a matter for civil litigation, criminal cases and national policy where fighting serious organised crime and cybercrime are concerned. The author, Brunella Longo, investigates this subject, suggests criteria and offers practical guidance for researching the issues. The article also includes references to relevant legislation, normative technical standards and best practices that have emerged as a result of corporate IT developments.
Keywords: mobile technology; wireless networks; cybercrime; information security

MOBILE AND EMBEDDED COMPUTING: THE LANDSCAPE REDEFINED

During the last two years 'bring your own device' or BYOD has emerged as the most pervasive and fastest growing phenomenon that corporate IT managers have had to deal with, together with wireless technologies and RTLS (real time location systems). The expression effectively refers to the current trend of employees and collaborators using their own laptop computers, cellular phones, smart phones, tablets (an Apple iPad, Kindle Fire, Google Nexus 7, to cite a popular few) both for personal and for work-related purposes, and accessing a potentially infinite variety of data and applications.

Brunella Longo

Another interesting term that frequently refers to a variety of tools used to communicate and share information with suppliers, customers and colleagues is mobile computing that sounds less fashionable but is, perhaps, a more precise and appropriate term. In fact, mobile computing suggests computing and storage capabilities of devices increasingly used, not just as a companion with limited functionalities, but as a powerful substitute of traditional desktop computing operations in order to process, distribute, access, store and manipulate data.

Furthermore, definitions of mobile devices tend to include other things that are easily connected to the internet or other private networks and which are used for data identification, storage, sharing and management. These devices include, for instance:

- Portable Universal Serial Bus (USB) devices for storage (such as MP3 devices) and for connectivity (such as Wi-Fi, Bluetooth and modem cards);
- Digital cameras;
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices;
- Infrared-enabled (IrDA) devices such as printers and smart cards.[1]

In all circumstances, mobile computing allows end-users to access computer networks in order to transfer, exchange and communicate via a phone, e-mail, text and, increasingly, through audiovisual formats. In a nutshell, the combined use of mobile devices and internet connections makes an employee able to telework, having remote access to an organisation's resources, and stay seamlessly

in touch with extended networks of personal and professional contacts.

WIRELESS NETWORKS: HISTORICAL CONTEXT

One central enabling technology associated with mobile computing is wireless networks. These allow mobile devices to establish, and use, an internet connection to access a local area network 'anytime, anywhere' (i.e. wireless), without the need for any physical cabling infrastructure.

The technology that has been developed to enable wireless connections has been developed around different standards and radio band services, the progenitors of which were those electromagnetic waves discovered and patented for the first time by the Italian inventor, Guglielmo Marconi at the British Post Office in 1895 and used in 1905 to send Morse coded messages across the Atlantic. Wireless local area networks (WLANs) are, most of the time, implemented and deployed using a specific family of standards known as the IEEE 802.11 and its numerous variants, successors and European or Asiatic counterparts and equivalents. However, these are not as stable, universal and safe as one would imagine.

When one looks back at the fascinating history of wireless technology with its military and commercial applications it seems almost unbelievable that it took until 2008 before the National Institute of Standards and Technology (NIST - http://www.csrc.nist.gov) publicly recognised, and extensively warned about, a lack of security in WLAN technologies and standards. A strong call for more security measures in order to prevent or to minimise unauthorised access to wireless network traffic, had in fact been made since World War II.

As often happens with innovations that radically change the way we communicate, when the first wireless LAN was adopted for computing purposes in 1971 at the University of Hawaii, the known risks of losing confidentiality, and the integrity of the data exchanged, via radio communications was simply underestimated or not even considered at all. At the time it must have been simply extraordinary to have seven different computers able to communicate with a central computer by using phone lines. IT security in a research context was almost irrelevant at that time.

SECURITY ISSUES AND STANDARDS

More than thirty years later, we have seen the inevitable consequences of that choice spread all around the security breaches existing in computer networks, affecting many IT infrastructures and industrial and commercial software systems.

In recent years good progress has been made by IT professionals and engineers in the development and implementation of better wireless standards following directions given by, among others, NIST. The last statement by NIST in 2008:

> *"Organizations employing legacy IEEE 802.11 WLANs should be aware of the limited and weak security controls available to protect communications. Legacy WLANs are particularly susceptible to loss of confidentiality, integrity, and availability. Unauthorized users have access to well-documented security flaws and exploits that can easily compromise an organization's systems and information, corrupt the organization's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use the organization's resources to launch attacks on other networks."*[2]

EMBEDDED COMPUTING APPLICATIONS

An accelerated pathway for the development of a more optimistic scenario for the security of mobile computing and wireless technologies is emerging from the advances made in the so called "embedded computing" applications, mainly based on RTLS (real time location systems) and sensors technology. In the energy sector, for instance, such developments foster more integration and convergence among diverse families of standards. These developments can more deeply innovate the fundamentals of cyber security required for the operation of smartgrids, defined as, "electrical networks merged with digital information systems"[3], and a wide range of telemetering, telecontrol or revenue metering applications.

The same, necessary level of certainty about the integrity and reliability of data transmitted through a WLAN is required to reach further levels of automation in transport or healthcare applications. In fact, digital signal processing is essential for the implementation of whatever type of embedded system. This is "a specialised computer system that is integrated as part of a larger system".[4] The optimisation of the security required at this level of the automation of data-sharing (among machines that control infrastructural and life critical applications) should also be beneficial for more common and trivial systems and software applications (like the smartphones and tablets impacted by the BYOD trend) within the next ten or fifteen years.

In the meantime, the usefulness of RTLS technology to the BYOD trend and to MDM (Mobile Device Management), in order to strengthen wireless networks capabilities, is still a matter of experimentation, partial successes, limited security and a large number of both critical and non-critical data leakages and confidentiality failures. It is not impossible that several organisations may wish to implement a BYOD programme as a controlled, though somewhat disruptive, strategy to innovate their own legacy and obsolete WLANs.[5]

https://doi.org/10.1017/S1472669613000285 Published online by Cambridge University Press

LEGAL ISSUES, CYBERCRIME AND CYBERLAW

Having examined some of the technical aspects of IT security, the author now wishes to turn her attention towards some of the legal issues associated with cyber crime. Crimes committed against, or through, computers tend to be divided into three categories:

1. Crimes against a specific computer, a network infrastructure or one of its components with the intention to steal data, modify and damage records, and/or vandalise technical equipment;
2. Crimes against individuals and organisations by means of their computers and through computer networks. Financial fraud, identity theft, credit card and telecommunications frauds are the main examples of this category;
3. Crimes that are perpetrated with the aid of data created, exchanged and stored through computer networks – for instance child pornography.

As far as the first two categories are concerned, and as Jahankhani and Beqiri identified, "Law enforcement investigators initially considered electronic evidence as any other type of evidence; however they realised soon that this was not the case and that the conventional approach was not suitable to collect, preserve, and analyse electronic evidence".[6] Many forensic processes have been abandoned during the last ten years while it has emerged in several countries that the only way to address certain types of cyber crime is through international cooperation. Hence, network forensics is still a very young and often weak discipline, the reliability of which is complicated in the common law countries by the absence of national ID cards and the propagation of antiforensic methods, particularly via wireless networks. "Antiforensics is the terminology used to define the activities of hackers and other cyber criminals aiming to undermine or mislead a computer forensic investigation"[7].

In the third category there are an increasing variety of frauds and misbehaviours; the more the digital economy becomes pervasive in the industrial and commercial sectors the higher the number of crimes supported by information that is created, stored and exchanged electronically. The differences between crime and cybercrime are virtually seamless but for the law enforcement possibilities.

From a legal and forensic point of view, mobile computing only exacerbates what has been the main problem in computer law and litigation involving computer networks. In many disputed situations the existence of legal obligations, the availability of specific legislation (such as the Computer Misuse Act 1990 in the UK or the entire Intellectual Property corpus) is not sufficient to bring a case to trial or obtain a positive judgment in Courts.

The point rarely taken into account by end-users, and indeed by IT security professionals and computer network scientists, is that there is no certainty about the legal direction regarding these issues because of the extremely uncertain relationship between the law and the facts which are often disputed. It is not because of a failure of the judiciary system; it is neither the failure of the law per se in relation to the internet nor because of an implicit failure of the technology.

Digital environments, or digital markets, are often characterised by vagueness and an ambiguity of the documentary evidence, even when software programmers and competent computer users seem to have almost absolute certainty about what has occurred. Conversely, even if the quality of data is crucial for the admissibility of evidence, documenting such a digital context may make a big difference. As Hart and McNaughton state, "for the most part, the law must settle disputed questions of adjudicative fact by reliance upon the ambiguous implications of non fungible traces on human brains and on pieces of paper and traces in the form of unique arrangements of physical objects".[8]

In several other circumstances it does not matter that there is a failure of digital forensic techniques, or a success of anti-forensic attacks, in framing a judgment. On the contrary, the crucial point is that an arguable, or disputed law makes it impossible to agree what is, or should be, considered the legal standard useful to shape a decision-making process. Hart and McNaughton wrote, "The 'legal standard' is what may be expressed in terms of ordinary human experiences and help solve the ambiguity. For instance it is unlawful (lacking due care) to attempt to pass another car when vision over the distance necessary to accomplish the passing is obscured".[9]

It is emerging that in cyber law, the notion of digital evidence that is likely to be accepted in court is not a super-technical *deus ex machina* that could be provided through digital forensic processes by technological means. Instead, it is just a "case-specific assertion of fact that must be probably true in order to lend support to a legal claim", no matter where (and how) it comes from or what the data is made of.[10]

In fact, there is a growing number of very relevant legal decisions - from the seizure of Hong Kong-based abusive Megavideo sites to the sentence of "unpatentability" of *Amazon 1 click* by the European Patent Office. There was also the recent UK case of defamation via Twitter, *Cairns v Modi* [2012] EWHC 756 (QB), which proved that the law is catching up fast. Several courts of law have found their way to weight their decisions against episodes of cyber crime with, or without, the support of specific or special digital evidences.

Theoretical studies and practical research about the state of cyberlaw is helping the debate that is influencing internet governance, the ideological positions that are impacting on political and policy matters and the views about the self-regulatory power of digital communities that, in turn, may have some influence in case law. Michael Froomkin (in the USA) and Chris Reed (in the UK) are among the law academics who have been suggesting for years that a new mindset, not just a new set of rules, is required to govern digital markets.

https://doi.org/10.1017/S1472669613000285 Published online by Cambridge University Press

CYBERCRIME: DEFINING THE SUBJECT FOR RESEARCH

To keep up efficiently with technological advances and the state of play with computer law, it is essential to identify and understand the progress made in procedural knowledge and technological standards that could impact on mobile computing from a legal point of view. As far as a subject approach is concerned I have defined six classes of issue that seem to be very relevant in the context of such technologies. Understanding these classes will help the researcher to discover a subject that is, at times, challenging to grasp.

1. Unintentional misconduct due to an error of judgment in relation to human behaviour;
2. Deliberate cyber crimes through innumerable digital techniques and media – anything from malware (malicious or malevolent software) and social engineering through to brutal computer hacking;
3. Influence and clash of local cultures and subcultures via social media and social networking sites leading to episodes of bullying, antisocial behaviours and other clearly provocated events or incidents;
4. Lack of governance and appropriate organisational measures such as accountability or requirements for compliance;
5. Immature, obsolete, flawed, wrong or forgotten technical standards in place without any maintenance or control;
6. Use of flawed, poorly designed or obsolete software application systems.

MONITORING DEVELOPMENTS

Public knowledge in relation to cybercrime and digital forensics is relatively limited and the subject is rarely shared and disseminated beyond those few specialists in academia. As a result the issues are less easily accessible for legal and paralegal professionals. Another problem is that the majority of the available literature is not translated into languages other than English. This has the detrimental consequence of a lack of sharing of expertise and knowledge for research purposes and, more crucially, for policing operations at international level. To address this particular problem, in 2009 the US Library of Congress's Federal Research Division produced an Annotated Bibliography under an Interagency Agreement with the National Institute of Justice (http://www.loc.gov/rr/frd/). This helpful resource covers studies published from 2000 to 2008 in Chinese, Dutch, French, German, Italian, Japanese, Korean (Republic of Korea), Russian, Swedish, and Ukrainian.

For the purposes of keeping up-to-date with developments in legal research, cybercrime and digital forensics, conference papers, grey literature and journal articles are the main sources. There are a number of particularly useful resources and platforms for this kind of research such as Engineering Village (http://www.ei.org) or the IEEE's Xplore Digital Library (http://www.ieeexplore.ieee.org). The Social Science Research Network (SSRN) (http://www.ssrn.com) or the abstracting and library service of the US National Criminal Justice Reference Service (http://www.ncjrs.gov) are also helpful; the latter has an excellent bibliographic collection with numerous and recently updated studies in digital forensics. Engineering Village offers access to the Compendex and Inspec databases via a common interface. With their historical collections these databases cover an infinite variety of technologies, and document their diverse stages of development. Inspec has an excellent interdisciplinary orientation that is very useful for legal studies and for understanding of the evolution of technical matters. For an understanding of the cybercrime phenomena and the political implications of legislative processes that pertain to IT, the internet and developments in the digital markets there is the *Worldwide Political Science Abstracts*, a database with coverage starting in 1975. Finally, the Electric Power Research Institute is a good reference resource to keep up with vendors' implementations and new developments of embedded systems in the Energy sector and related cyber security findings (http://www.epri.com).

CORPORATE IT CASE HISTORIES

Best practices in the corporate sector are emerging from early adopters of Mobile Device Management (MDM) solutions. Such IT developments are regularly covered by professional and trade magazines indexed and stored by EBSCO Business Source and other similar databases. Case histories offer the opportunity to benchmark the implementation of existing standards in diverse organisational contexts and sizes and across sectors. These case histories involve some prominent companies such as:

- Safety Insurance Co
- Meadowbrook Insurance Group
- Pabst Brewing Company
- The Northern Star Council of the Boy Scouts of America
- Sainsbury's
- MasterCard
- Deloitte
- Canon
- Electronic Arts (EA).

MasterCard and Electronic Arts may seem very surprising in that the former was the first to exclude corporate Blackberrys from the BYOD programme and the latter, a company active in the electronic games industry, decided to allow only 10% of employees use of personal devices on the job. These two examples demonstrated that such case histories are unlikely to be universally significant or representative of particularly effective, or resolutive, technical solutions to WLAN security problems. On the contrary, most organisations view the BYOD trend as

https://doi.org/10.1017/S1472669613000285 Published online by Cambridge University Press

dependent on the management of information interaction both at individual, and at organisational, levels, via very tailored and personalised solutions.

CONCLUSIONS

Naturally, people want to use their own devices for work-related purposes because it is often their quickest, most pleasant and effective option. It allows them to be in control of their own agendas, reducing personal information overload, optimising the cognitive effort required to be multitasking and provides opportunities to find a better work-life balance.

That situation occurs in a context that is far from being under the total control of an IT department, no matter how well managed the security aspects are in relation to BYOD initiatives in the workplace. Instead, the organisational context is often invisible, mutable and without the necessary security warnings. It is essentially unmanageable in all its possible layers. As Tefko Saracevic once stated, "context is not self-revealing, nor is it self-evident. Context may be difficult to formulate and synthesize. But plenty can go wrong when not taken into consideration in interactions."[11]

Technologies associated with information and communication proliferate new applications that are appreciated by end-users of mobile devices. The expansion within the creative industries and entertainment markets things are moving at a fast pace. This is causing corporate decision-makers to design BYOD experiments and policies and to introduce MDM solutions. Conversely, awareness of the overall technical inadequacy of current WLAN standards to completely secure mobile computing usage, is growing very slowly and there is some urgency for a renaissance of authentication technologies and network forensics.

It is also true that social optimisation of very widely adopted technological innovations, requires a long time to develop. For instance, and by comparison, it took more than one century for the electricity sector to reach the level of regulation, honing of standards and wide social acceptance of the legislative measures that it has now. The IEE Wiring Regulations reached its 17th edition in 2011 while the first Act relating to electric lighting meant for the prevention of fire risks and electroshock was passed by the UK Parliament in 1882. Mobile and embedded computing requires the same level of business certainties, quality assurance, compliance and enforcement possibilities available for the physical wirings regulations. Contributions from legal research and practices to this development process should be considered a priority and looked at with favour.

Footnotes

[1] ISACA. (2010) Securing Mobile Devices. An ISACA Emerging Technology White Paper.
[2] NIST. (2008) Guide to Securing Legacy IEEE 802.11 Wireless Networks. Special Publication 800–48 Revision 1.
[3] Hadjsaid, N. and Sabonnadiere J-C. (2012) SmartGrids. Wiley.
[4] Kleidermacher, D. and Keidermacher, M. (2012) Embedded Systems Security: practical methods for safe and secure software and systems development. Elsevier.
[5] Longo, B. (2013) Mind the BYOD gap. Cybersecurity at a crossroads. Self-archived version available through http://www.SSRN.com.
[6] Jahankhani, H. and Beqiri, E. (2008) Memory-Based antiforensic tools and techniques. *International Journal of Information Security and Privacy*, 2 (2) pp.1–13.
[7] Ibid
[8] Hart, H. M. Jr. and McNaughton, J. T. (1958) Evidence and Inference in the Law. Evidence and Inference. The Hayden Colloquium on Scientific Concept and Method. The Free Press of Glencoe, pp. 48–72.
[9] Ibid
[10] Schwartz, D. S. (2011–2012). A Foundation Theory of Evidence. *Georgetown Law Journal*, (100), 95–172.
[11] Saracevic, T. (2010) The Notion of Context in "Information Interaction in Context". IliX 2010, August 18–21, 2010, New Brunswick, New Jersey, USA.

Biography

Brunella Longo is a consultant with an expertise in design and project management of innovative information services. Brunella worked for 13 years in library, documentation and intelligence roles, including the provision of legal information services, before setting up, in 1995, her first consultancy and training business in Milan (Italy) supporting internet, digital, bibliographic and e-learning projects until 2008. In 2011, after several charitable activities that kept her busy for two years, she re-started her consultancy in London where she found further motivation to investigate cyber security and information assurance for digital markets. Brunella is an author of three books and many articles, training materials and conference speeches on information management issues.

https://doi.org/10.1017/S1472669613000285 Published online by Cambridge University Press