Who Owns *My* Device?

A. A. Adams

Centre for Business Information Ethics, Meiji University
1-1 Kanda Surugadai, Chiyoda-Ku, Tokyo-To, 101-8301, Japan
Phone: + 81 332964545
aaa@meiji.ac.jp

Abstract

Ownership is a shorthand that philosophers and lawyers use to represent a bundle of rights. These rights are not eternal and are particularly subject to change due to technological development. To most individuals, ownership implies a very broad set of rights. When we buy the latest computational devices such as smartphones and tablet computers, these rights seem to have disappeared and instead the user is faced with entering a state of feudal dependence on the goodwill and honesty of the manufacturer, the vendor and the Internet connection service provider. In this article, the history of rights in connected and standalone, shared and single-user, devices is compared to the current state of ownership in smartphones, tablets, laptops, desktop computers and cloud services. The implications for privacy and security are also explored.

Keywords

Smartphone, Tablet Computer, Ownership, Privacy, Security

INTRODUCTION

Ownership is one of the key foundational ideas of political theory. Mill (1852) defines ownership as a consequence of the rivalrous nature of a resource or property, which can be inherent or induced by law. When a resource is limited in its availability for use, in order to avoid the War of All Against All suggested by Hobbes (1651) as the natural state of humanity without enforced obedience to a sovereign. Ownership is not an absolute and unbounded right over the owned property, but is recognised in law and philosophy as a bounded set of rights, sometimes also bringing with it obligations.

In modern times it is not only land and physical objects which are owned, but concepts, connotations and identities. Despite the protestations of Jefferson (1907) that there should be "No Patents on Ideas" allowed by the Constitution of the United States of America (argued, inter alia, because "If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea,…") patents, copyright, trade secrets and other laws are not only part of the US Constitution and statutes but are the subject of some of the broadest harmonised legal instruments in the world, through various international treaties such as the World Intellectual Property Organisation (1996) Copyright Treaty.

In addition to setting minimum (but not maximum) harmonised rules on issues such as the length of copyright protection to be provided to authors of books, computer programs, musical compositions and recordings, and audiovisual works, this treaty requires signatory states to (World Intellectual Property Organisation, 1996, Art 11):

> provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

The implementations of this treaty in national laws, such as the Digital Millennium Copyright Act (Congress, 1998) in the US, have been heavily criticised for their implications for general purposes computing devices and software ideas, particularly in the area of Free Software (Williams, 2002). They also formed the basis for lawsuits (and other legal processes such as rulings by the US Copyright Office (Lee, 2012)) regarding the rights of purchasers of electronic devices to modify the hardware or software in ways objected to by one or more of the providers of the device. By provider, we include the manufacturer[1] but also others such as mobile telephone service providers who supply customers with both devices and connectivity service. When a customer purchases most physical goods, such as clothing, furniture, crockery, jewellery etc. they expect that their purchase provides a broad ownership of the item. These expectations include rights (subject to general lawful behaviour) to:

- use the item at times and places of their choosing — neither to be required to use the item at specific places nor denied the right to use it at specific places or times;
- modify the item, providing the resulting item is not inherently dangerous;
- resell the item, at whatever rate the market will bear, and transferring all rights on to the subsequent owner
- use the item in any way that the owner can conceive of employing it, whether or not that use was intended or even conceived of by the creator/provider.

However, the growing reality with respect to modern information and communication devices is that users are highly constrained by both technical and legal barriers to their exercise of these kinds of expected rights. The law in this area is still very much in development with many contradictions and difficulties, and even where users' actions are determined to be legal very often the technological barriers placed in their way are accepted by legislators and courts as also legal. In this paper the development of the concept of ownership of information and communication devices is considered, together with an analysis of the market, social norms, technological architecture and

[1]In the modern global economy, few devices are solely manufactured by a single firm. Apple Inc. for example designs their iOS devices (iPod Touch, iPhone, iPad etc.) and produces most of the operating system software but outsources the physical creation of the devices and its components and brings in by various means certain parts of even the core operating system from other sources.

legal structures surrounding the complex question of "*Who owns my device?*", that is: what rights does a purchaser have in law and reasonably have the facilities to exert, when they purchase a computer, smartphone, tablet, game console, etc.; do these rights fit with consumer expectations when they pay for these devices (and have a belief that they own them); with the growing convergence of devices and bundled services, what is the future of corporate and personal rights over devices and the data they process.

THE EVOLUTION OF MACHINES

Modern information and communication devices are converging from separate forms to overlapping and converged forms. Modern mobile telephones have gradually become pocket-sized, one-hand touch-screen interface mobile networked computers which also include telephone services. Personal Computers now come in shapes from handheld clam-shell devices through tablet/phone hybrids, laptops, mini-servers and desktops. Mainframes and racked servers compete for the provision of large-scale computing resources but the Internet and high speed networking has removed the need for their physical placement within corporate premises and flexible cloud computing now makes variable-scale computing resources available to the largest companies and individuals on an equal footing (except for ability to pay, of course). The evolution of these machines has been paralleled by the development of expectations, rules and laws about their use.

Early Computers

In the early days of computing the machines were owned by research institutes and governments and dedicated to the work of their organisational owners and for research into computing. As the age of business computers developed, these were again primarily organisationally owned and the original mainframes had usage strictly controlled by high priests accepting batch jobs submitted on punched cards and dispensing the results (or, with a disapproving mien, the error messages) of the computation. The advent of the mini-computer, and real-time interactive systems led to the opportunity for a broader class of users to access these machines (Levy, 2001). The beginnings of modern computer security questions then emerged, such as the requirement to restrict access to one's computer account with a password, objected to by Richard Stallman (Levy, 2001, p. 417):

> I suggest that you switch to the password "carriage return". It's much easier to type, and also it stands up to the principle that there should be no passwords.

While Stallman's crusade for Free Software (Williams, 2002) has become a worldwide movement that competes with (and in some areas defeats) the proprietary world of most software, the open access principle of no passwords has gone. Stallman's idealistic notion of 1977, described by Williams (2002, pp. 53–54) as "…the hacker notion that [MIT AI] Institute computers, and even Institute computer files, belonged to the public, not private individuals." seems a quaint and bizarre viewpoint in the world of Anonymous (Walker, 2012), Wikileaks (Hood, 2011 ; Benkler, 2011) and online banking, Stallman's carriage return password philosophy was still based on question of

ownership of information, ownership of the machine, rights to access information (and to delete or change information, including the operation of programs).

Early Telephones

In the UK fixed line telephone services were a (state-owned) monopoly until 1984 (Armstrong, 1997) (when it was privatised and a single license given to Mercury Communications creating a duopoly of two private firms until 1990). In addition to the telephone service, BT generally provided the equipment which attached to the network in the home charging a separate rental fee for the equipment. Only once this monopoly was removed did the user-friendly "in-phone" socket become the usual in-home connection, allowing personal equipment to be easily plugged into the telephone socket. Previously, equipment had to be directly wired in to a "bayonet" attachment, and the BT terms of service required this to be performed only by BT personnel. Similar provisions were used by AT&T, with regulations that permitted only equipment approved by them to be connected to their telephone network (Olley & Pakes, 1996), a stance which was gradually whittled away but not entirely removed by first the Hush-a-Phone[2] and Carterfone[3] cases.

In both cases, the provider of a network service used the excuse of potential damage to their network to remove the possibility or scope of competition for providing equipment to consumers, ensuring their own monopoly on consumer purchases or rental of a subsidiary market.

Personal Computing

The development from the mid-70s onwards of first the minicomputer, then the personal computer, led to the physical ownership of computers by significant numbers of people. They also led to many people being supplied with individual computers by their employers, at individual desks and dedicated to their own use, in their own home and then as portable devices capable of being carried around between work, home and in fact almost anywhere else. The limitations of networking in the early days led many of these machines to store significant amounts of data on the local hard drive and/or on the fragile removable media (often transferred to other machines via such media, sometimes referred to as sneakernet (www.catb.org/jargon/html/S/sneakernet.html)). The localised nature of the data processing and storage capacities of these machines, combined with their usage being dedicated to individuals, led many to develop a sense of ownership even towards employer-owned resources. Indeed, this appears to be a fundamental facet of human psyhology, as demonstrated by Reeves & Nass (2002) in whose work it is reported that many college students would wait around until their preferred machine became available in a computing lab rather than

---

[2] 238 F.2d 266; 99 U.S. App. D.C. 190; 1956 U.S. App. Hush-a-Phone was a physical device which fitted an AT&T telephone receiver's microphone to reduce the potential for s bystander overhearing, which coincidentally also improved the pickup sound quality by reducing extraneous noise.

[3] 13 F.C.C.2d 420 (1968); 13 Rad. Reg. 2d (P & F) 597

use a fungible different machine (the hardware and installed software being identical and the student's files being held on removable media or a network drive equally accessible from each machine).

Company policies and employee compliance varied, although there were some emergent accepted ethical standards, such as those reported by Conger et al. (1995) including the unacceptability of gaining profit from use of employer resources for non-employer remunerated tasks, the inappropriateness of use of employer resources for sexual purposes, but the acceptance (by both employers and employees) of some social use of employer resources, particularly non-consumable resources for non-profit purposes during employee break time.

Personal computers then became more personal as people starting buying their own at home in large numbers. These home computers were used by many for some work-related tasks. This sometimes required specific software to be installed on the machine. The results of work might be transferred by sneakernet or as printout or simply in the employee's head. Sometimes software purchased by the employer was needed to perform this work. Employees would therefore install the needed software from physical media borrowed from the workplace. Sometimes this was with the knowledge and permission of the employer and sometimes not. Sometimes it was within the software license held by the employer and sometimes not. Business software licenses have a number of forms, including a maximum number of machines on which the software can be installed, or a site license covering all machines owned by the company, or all machines present at a particular location. The location licenses were tricky to comply with once laptop computers became common since such licenses were often unclear whether this covered machines sometimes present in the building and sometimes not. The increases in network facilities were used by software vendors to try and apply technological measures to ensure license compliance. One method of applying limitations was to have a license server running on a network which would authorise installed copies of software to execute only if there was a spare license. As Internet connectivity became more common, it was no longer necessary to restrict such licenses to a particular location, but they could be issued to anywhere. This allowed employers to permit the installation of such licensed software on employee's home machines without violating their software licenses.

Networking of Computers

As mentioned above, in places of work and study, networked storage facilities gradually emerged to allow for various benefits to both the employer and employees, such as the easy shift to another machine (either in a different location or replacement of the machine on one's desk), access from other locations around the workplace, simpler backup facilities etc. As home Internet connectivity became first affordable for employers to provide to employees, and then cheap and desirable enough that employees paid for their own service, teleworking became feasible for a broader class of knowledge workers than before. Employers providing computers and paying for Internet connections in the employee's home had to make a choice about how to treat personal usage. Such facilities are not the only ones employers (and tax authorities) have had to consider in regards to

policies surrounding personal employee use of employer resources. If an employee drives a company vehicle, are they permitted to use it for personal travel? Is specific permission required for each use? Does diverting a few hundred yards to drop in at the grocery store on the way home count as personal use? Driving hundreds of miles on a weekend family trip almost certainly would. What costs does the employer incur by allowing such personal use? In the case of company vehicles this depends on whether they pay for consumables such as fuel and on the extra depreciation of the asset, and on insurance coverage costs. Tax codes take these things into account and often regard personal use of a company resource as a taxable benefit to the employee.

In the case of computers the depreciation of the asset due to extra use is tiny (consisting more of an increased likelihood of early failure of certain components like hard disc drives) and unless the Internet connection is billed on a volume transferred or time connected basis, rather than a monthly subscription for unlimited data transfer, then use of the Internet connection for personal use has no financial implications for the employer. However, allowing personal use of the computer and network connection has non-financial implications. The personal use made by the employee may involve illegal activity, or activity which is legal but with which the employer may not wish to have any association. This latter can include access to sexual information, for example, or the posting on a personal blog of criticisms of the employer, the employer's customers, etc. Depending on the employment law in the relevant jurisdiction, an employer might be able to terminate the employee's employment for such actions whether or not they are performed using employer resources or during work time. In the US, for example, a waitress was fired for posting a picture of a customer's receipt online (Weisenbaum, 2013), while in the UK a shift manager at a public house was dismissed for posting derogatory comments on her Facebook account (while still on shift) about customers who had been abusive.[4]

Smartphones

The smartphone, a fuzzy category of devices that are thought by some to start with the iPhone but by others to have been around since the first Blackberry and Nokia devices which provided Internet email connectivity on the phone itself, is now well-established and although still a minority of mobile phone sales in the final quarter of 2012 (IDC, 2013) is approaching 50% of new sales. These devices have brought into sharp relief the questions already posed by computers and network connections, but also brought new elements into play. Broadband Internet connection providers, unlike earlier walled-garden services such as AOL and Minitel, have generally provided a neutral net connection available through a standard network interface[5] these days generally a wired ethernet and/or wireless WiFi connection. New machines, or new operating systems, can be added to those

[4]UK Employment Tribunals Case Number: 2104806/10 uk.practicallaw.com/6-505-8064?q=preece.

[5]AOL is unusual in that although they provide Internet connectivity, they still require a proprietary program running on a limited set of operating systems to perform authentication onto their system even where only Internet access is needed.

networks without limitation using network address translation which allows one machine connected to the Internet to act as a bridge for other machines on the same local network. However, mobile telephone service providers are far more restrictive in their service offerings, often doing their best even when providing a supposedly unlimited volume data connection to restrict usage of that connection to only the specific device they provide.

Apple's iOS-based iPhones and Android-based phones from a variety of makers dominate the smartphone market, sharing over 90% of sales in the final quarter of 2012 (Gartner, 2013). As discussed below, while the two platforms iOS and Android have some significant differences in approach and levels of openness, they are both to subject to restrictions by various companies, particularly including the mobile service providers who usually act as retailers. Despite paying for the physical device, either at provision or via a monthly addition to the service subscription, many phones, including smartphones, may be locked to provide service only to the carrier which sold it and provided the initial service for it. This issue alone raises a fundamental question about ownership. If a customer has purchased a device which is technically capable of connecting to any network, save for the deliberate blocking of this capability by the service provider. Some of the software installed on smartphones may be impossible to uninstall, or even impossible to prevent it running, even when that software has no connection to the necessary operation of the phone or its interaction with the network. iOS phone are initially locked to prevent installation of software from any source other than the Apple App store. While most Android devices allow the installation of apps from sources other than some default(s) (set first as Google Play (previously Android Marketplace) but sometimes overridden to their own store by handset makers and/or vendors), some devices have or have had this feature locked off (such as AT&T until 2011 (Electronista, 2011)).

Virtualisation and Cloud Services

Virtualisation has been a common practice in certain elements of computing for decades. IBM, and compatible systems offered by competitors such as Amdahl, offered the option (or later, sometimes only) of the main system running the machine primarily working as a host for virtual machines. These virtual machines, hardware emulated as a software layer, appear to the user as their own machine. So long as it has been compiled for the hardware being emulated, any operating system can be run on a virtual machine.

Virtualisation has existed as a relatively modest background element of computing for decades but it recently gained much more prominence on both the large and the small scale. At the small scale the improvements in hardware power and in virtualisation efficiency (using as little processing power and memory as possible to run the underlying system, thereby freeing up the power of the machine for the target process) meant that a well-known security paradigm of separating applications each into their own virtual machines (preventing those programs from accidentally or maliciously interfering with each other) and only allowing them to interact via properly defined interfaces. At the large scale the demand for flexible computing power, flexible storage space and flexible download bandwidth has led to the development of Cloud Computing where the exact

location of one's data and processing mostly does not matter to the provider of the data or its users. It only mostly does not matter, since the location of the server, the registered headquarters address of the hosting company, or even whether that company has significant operations in a country, could potentially place users' data and usage details under other jurisdictions (Gallagher, 2013). While data placed on a cloud storage service can be encrypted by the user and depending on the strength of the encryption used this can be fairly secure, anything processed on a cloud server will generally need to be unencrypted for the processing to happen. Even if communication between the service user's local machine and the cloud provider is encrypted, governments can sometimes force the provider to allow access.

HARDWARE, SOFTWARE, DATA

Ownership of devices (hardware) is only one of the tricky issues facing society with regards to the Information Revolution (Castells, 1996). As mentioned above, computer software also provokes tricky questions with regards to the limitations on the use of software (and associated activities) that can be placed on users by software producers, and on the limitations of what software producers may do with respect to the hardware on which it is installed, and with any data on that machine that is visible to the software. Software can be considered simply a class of data — functional data, perhaps – and the question of ownership of other data is a further tricky question. In the case of commercially produced and distributed entertainment data, educational data and personal data, various laws (copyright, human rights, data protection) and ethical viewpoints also come into play. While a broader discussion of the ownership of data is beyond the scope of this article, it should be noted that the practical exercise of rights with regards to data (functional or not) can be heavily constrained by the rights over the machine on which that data is placed.

OPEN AND CLOSED PLATFORMS

Home and office individual computing equipment has seen a variety of levels of openness over the years with a range of successful strategies. The IBM PC has been an open platform almost from the beginning. The hardware was designed to allow third party hardware to be added via standardised ports internally and externally to the base machine, and the hardware was also designed to allow software by multiple vendors to be run as an operating system. These operating systems were also designed to allow anyone to install and run programs.

Game consoles, on the other hand, have always been jealously closed systems often with limitations on what hardware can be added, and almost always with software restricted to that provided by or via the platform manufacturer. Sony, for example, have gone to court in many countries in efforts to prevent the provision of (and/or installation of) modification chips (mod-chips in the parlance) which bypass their restrictions on software. They claim this is to prevent unauthorised copies of the games they provide being played (a stance often supported in law) but opponents have argued that it also prevents official games bought in some countries from being played on consoles bought in others (allowing differential pricing for the same game, despite globalised retail options now

available to the consumer) and preventing users from running software developed without Sony's approval, but legitimately supplied to consumers, from being run. So far Sony have mostly prevailed in their court cases.

In an interesting contradiction, however, the US Copyright Office ruled that bypassing software restrictions on Apple iPhones was legal (and by extension, other equivalent devices such as Android smartphones). The US Copyright Office further muddied its own decision, however, by differentiating between smartphones and tablets in a further decision, although not withdrawing their decision surrounding iPhones. A further twist emanating from the US Copyright Office came in late 2012 when it reversed a previous decision making it legal for owners of cellphones to break the network locking applied by many, though not all, US mobile network operators to cellphones sold with service contracts.

Smartphones and tablet computers, whether from Apple running iOS, various makers running Google's Android, Blackberry's BlackberryOS or the various offerings (primarily Nokia and HTC) running Microsoft's Windows Phone, are fairly closed platforms. Apples iOS, Microsoft Windows Phone and Blackberry's Blackberry OS are all generally highly locked systems, with only the official App store of the software maker allowed as the source of new software. Only by breaking the security of the system could alternative sources of software be added, including locally available files - even programs written by the phone owner themselves can not be installed. Android by default has a slightly more open system, with a standard option of the system (but off by default) being to allow software to be installed from Unknown Sources, i.e. everything except Google Play on a default Android machine. Manufacturers such as Samsung can and do supplement or replace Google Play with their own known sources, as can and do mobile network service providers who sell tied phones. As mentioned above, a few mobile carriers have or continue to lock out that option from users. The ability to install applications from any source is one thing and allows amongst other things users to write and install their own software (if they have the programming skills). Full control of the phone or tablet is another matter however, and an Android device can still include unwanted applications, which may be run at startup, impossible to switch off, and have access to user data such as contact lists, location data, calls made.

While there have been attempts to improve the privacy and security model on Android in particular, one of the problems is that applications such as TISSA by Zhou et al. (2011) can only run in privileged administrator (root in Android terms derived from Unix) mode and so cannot be installed by ordinary users. Only manufacturers can install such software without themselves cracking the restrictions on administration-level access, for most devices, particularly for smartphones. Some manufacturers provide official administrator-level access tools, more commonly for tablets than for phones.

OWNERSHIP AND CONTROL

The old saying goes that "possession is nine tenths of the law" but in terms of electronic equipment, it is increasingly the case that the possession in question resembles medieval demons inhabiting

one's phone rather more than the physical holding of the device. Whether the device runs iOS, Android or one of the other less common systems, most are tricky on which to gain full control of the software. Unlike the IBM PC, there isn't a simple "boot from user-controlled source" system available for most, and many are strongly locked down to prevent users from even uninstalling some unwanted software or installing software from "unapproved sources". Apple were recently granted a patent on a method to remotely disable some features of smartphones such as the camera as reported by Whittaker (2012).

There are some bright spots in this area, such as the previously-mentioned US Copyright office ruling that "jailbreaking" (i.e. gaining full administrator control) over an iPhone is exempt from the Digital Millennium Copyright Act technological prevention measures circumvention ban. The refusal to extend the same principle to iPads and other "tablet" computers due to the "ill-defined nature" of tablets (Lee, 2012) is worrying, however, and the reversal of their previous decision on unlocking phones for use on alternative carriers is a move against consumer freedom and in favour of provider control. The US Copyright Office has clearly been influenced by concern over inconsistency with court rulings on bans on the sale or installation of modification chips in home games consoles, particularly Sony PlayStations (Fitzgerald, 2005), specifically citing handheld video gaming devices (for example the Sony PlayStation Portable and PlayStation Vita) as being devices which are close to tablet computers.

Personal Use of Company Machines and BYOD

Employers who provide machines to and/or pay for connectivity for their employees, whether that be desktop computers, laptop computers, tablet computers or mobile phones, may, as previously mentioned, explicitly allow the use of that equipment/connection service for personal use. Employees have also used their own devices, previously mostly desktop and laptop computers but now increasingly tablets and smartphones, for business purposes and in particular to connect to employer networks. The "Bring Your Own Device" (BYOD) issue has received significant coverage in the professional computing press and academic literature over the last few years, including on issues such as personal device use by students in schools and universities (Indiana State University, 2012), the impact of employee's/students personal device usage on organisational purchase of computers (ZDNet, 2013; Keizer, 2013), and the risks to organisational information security of BYOD (Mansfield-Devine, 2012).

Whether using company-owned machines for private purposes or using personal machines for work purposes, individuals' use of those machines is likely to be subject to restrictions by their employer. As discussed above, even personal use of personal machines on personal time can be subject to the threat or actuality of sanctions and even dismissal in the workplace. While many of the cases to date have involved the discussion or reporting of work issues, the question of company reputation reflecting from the private lives (now lived potentially in the public view for everyone on-line) of employees is also raised. Legal but unusual personal activity, often but not always in the sexual sphere such as involvement in dating sites, online exhibitionism, consumption of online erotic

material etc. can all be viewed negatively by some and risk-averse companies may seek to have and enforce codes of online conduct for their staff far beyond what would have been the case before the rise of the Internet. When the machines used have some direct connection with the workplace, this increases the options for employer surveillance, of accidental discovery of violations of policy and the reputational connection with the employer.

Security, Privacy and Ownership

Mulholland et al. (2006) described at length the challenge that service-oriented architecture and customer-driven engagement could and should create in enterprises. In particular they identified the challenges that allowing customers to access corporate information systems in a more interactive way than just reading corporate web pages or ordering from a fixed set of items in the catalogue of an etailer. One aspects that they did not cover was the reverse risk to consumers of lack of good faith dealings by enterprises with individuals, whether they are employees, customers or third parties.

One of the claims made by Apple regarding the benefits of the iOS family of devices is that the restriction of software sources 1 prevents the spread of malware. Unfortunately there are two flaws in this argument. The first is that malware-infected apps have appeared in the Apple App Store despite the checking Apple claim to do on all applications. The second is that iOS devices are subject to attacks through data downloads not just programs. Visiting the wrong website with the browser on an iPhone or iPad can lead to the machine being compromised. A sophisticated attack will gain access to the device at the administrator level. The Apple App store itself has until recently been critically flawed in its Internet connection process, leaving users open to infection when using open WiFi connections particularly (Goodin, 2013). These vulnerabilities are exactly the same as those used to jailbreak the iOS device, i.e. for the user to gain administrator rights for themselves. Users who have not jailbroken their devices are in a very difficult position if their device is compromised since their lack of administrator privileges makes it harder for them to detect or destroy malicious software. Android devices are just as vulnerable in this respect. Users who allow software to be installed from “unknown sources” are perhaps at slightly greater risk, but again once an attack succeeds in gaining root privileges on the Android device, for most users it can be hard to detect or destroy.

Schneier (2012) refers to the model of iOS and many Android devices as feudal security. In return for restrictions on their freedoms users expect to receive greater security. For users, this expectation of security would typically include protection of their privacy from at least third party developers and probably from the feudal overlord themselves to a great extent. Unfortunately, while not even receiving that much in the way of security benefits, the lack of control granted to users extends to the privacy model for applications on both Android and iOS devices, which have a highly coarse-grained permissions approach. Apps approved for distribution by the major App Stores including Apple App Store, Google Play, the Amazon App store for Android etc. automatically identify which types of data on the device an app accesses (this is possible because of the limited

development environment for these devices which defines specific ways to access things like the phone status, camera etc). There is no option to forbid certain types of access while still installing an app — users must allow all accesses requested or not install the app. Further, once an app has access to the data — say the user's contacts list, there is limited scope for automatic analysis of what is done with that data. If an app has access to the user's contacts list and to outgoing network communications (of any sort - even the right to open the web browser consists of an outgoing data connection and data can be embedded in outgoing URL requests) then apps have the technical capability to send that data out of the device. There are few or no tools made available to ordinary users by Apple, Google or the other operating system makers to allow them to monitor applications for such malicious behaviour. While apps are routinely pulled from various App stores for violation of privacy guidelines, the regularity with which this is happening shows that claims to pre-emptive security and privacy for users are far from accurate. in return for their loss of freedoms, it would appear that users are getting no more than the sign and semblance of their security.

CONCLUSIONS

Eminent domain is being exerted private actors in the overlap between physical property and the abstract world of information. This is being done with little concern for a serious debate over the rights of consumers and the potential real harm to networks (i.e. to the rest of the consumers) but is instead all about protecting the bottom lines of the handset vendors, the mobile phone network operators and those selling software to run on these machines. In the meantime it leaves users with various unpalatable options:

- Accept the risk of unscrupulous software vendors capturing one's device, invading one's privacy, and those of one's contacts, and even potentially running up unauthorised bills;
- Breaking the law and running the risk of breaking an expensive device ("bricking it", i.e. turning an expensive piece of electronics into nothing more than a heavy lump of metal and plastic) by illicitly bypassing the ownership restrictions;
- Not having access to high quality machines and/or reasonable connection rates.

On previous experience it is doubtful whether enough consumers will be willing to take the final route to force the market to adapt its practices, nor is there much hope that lawmakers will stand up for the information rights of their constituents against the lobbying of the network operators and handset hardware/software vendors who are amongst the world's largest corporations. Digital rights activist organisations raising the questions with the public and making it a serious regulatory issue, and where available pursuing cases to constitutional courts are the avenues which seem to be open at present.

REFERENCES

Armstrong, M. 1997. Competition in Telecomunications. Oxford review of economic policy, 13(1), 64–82. eprints.ucl.ac.uk/15114/.

Benkler, Y. 2011. A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate. Harvard civil rights-civil liberties law review, 46, 311–397.

Castells, M. 1996. The rise of the network society. The Information Age, no. 1. Chichester: Blackwell.

Conger, S., Loch, K. D., & Helft, B. L. 1995. Ethics and information technology use: a factor analysis of attitudes to computer use. Information systems journal, 5(3), 161–183.

Congress, US. 1998. Digital Millenium Copyright Act. H.R. 2281.

Electronista. 2011 (6 May). AT&T finally allows non-Market apps on Android phones. www.electronista.com/articles/11/05/06/att.allows.non.market.apps.on.infuse.4g.onwards/.

Fitzgerald, B. 2005. The Playstation Mod Chip: A Technological Guarantee of the Digital Consumers Liberty or Copyright Menace/Circumvention Device? Media and arts law review, 10, 89.

Gallagher, R. 2013 (8 Jan). U.S. Spy Law Authorizes Mass Surveillance of European Citizens: Report. www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html.

Gartner. 2013 (13 February). Gartner Says Worldwide Mobile Phone Sales Declined 1.7 Percent in 2012. www.gartner.com/newsroom/id/2335616.

Goodin, D. 2013. After leaving users exposed, Apple fully HTTPS-protects iOS App Store. Ars Technica, 10 March. arstechnica.com/security/2013/03/after-leaving-users-exposed-apple-finally-https-protects-ios-app-store/.

Hobbes, T. 1651. Leviathan: Or the matter, forme, & power of a common-wealth ecclesiasticall and civill. Indianapolis: Hackett.

Hood, C. 2011. From FOI World to WikiLeaks World: A New Chapter in the Transparency Story? Governance, 24(4), 635–638.

IDC. 2013 (24 Jan). Strong Demand for Smartphones and Heated Vendor Competition Characterize the Worldwide Mobile Phone Market at the End of 2012. /www.idc.com/getdoc.jsp?containerId=prUS23916413.

Indiana State University. 2012. BYOD: Embracing Technology in K-12 Schools. cacm.acm.org/careers/157358-byod-embracing-technology-in-k-12-schools/fulltext. Article in Online Communication of the ACM Career News section.

Jefferson, T. 1907. Writings of thomas jefferson (edited by a. e. bergh). The Thomas Jefferson Memorial Association.

Keizer, G. 2013. BYOD, for Buy-your-own-device, dampens corporate PC purchases. Computerworld, 29 May. www.computerworld.com/s/article/9239585/BYOD_for_i_Buy_i_your_own_device_dampens_corporate_PC_purchases.

Lee, T. B. 2012. Jailbreaking now legal under dmca for smartphones, but not tablets. Ars technica, 26 October. arstechnica.com/tech-policy/2012/10/jailbreaking-now-legal-under-dmca-for-smartphones-but-not-tablets/.

Levy, S. 2001. Hackers: Heroes of the computer revolution. London: Penguin.

Mansfield-Devine, S. 2012. Interview: BYOD and the enterprise network. Computer fraud & security, 2012(4), 14–17.

Mill, J. S. 1852. Principles of Political Economy. Vol. 1. Standard Library Company.

Mulholland, A., Thomas, C. S., Kurchina, P., & Woods, D. 2006. Mashup corporations: The end of business as usual. Evolved Media.

Olley, G. S., & Pakes, A. 1996. The Dynamics of Productivity in the Telecommunications Equipment Industry. Econometrica, 64(6), 1263–1297. econweb.umd.edu/~haltiwan/olley_pakes.pdf.

Reeves, B., & Nass, C. 2002. The Media Equation. 2nd edn. Stanford: CSLI.

Schneier, B. 2012 (3 December). Schneier on Security: Feudal Security. www.schneier.com/blog/archives/2012/12/feudal_sec.html.

Walker, J. 2012. Unmasking anonymous. ITNow, 54(1), 28–29111.

Weisenbaum, H. 2013. Applebee's waitress canned after posting pastor's tip. www.nbcnews.com/business/applebees-waitress-canned-after-posting-pastors-tip-1B8198406.

Whittaker, Z. 2012. Apple patent could remotely disable protester's phone cameras. ZDNet, 4th September. www.zdnet.com/apple-patent-could-remotely-disable-protesters-phone-cameras-7000003640/.

Williams, S. 2002. Free as in freedom; richard stallman's crusade for free software. Sebastapol, CA: O'Reilly.

World Intellectual Property Organisation. 1996. Copyright Treaty. www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html.

ZDNet. 2013. Byod and the consumerization of it. www.zdnet.com/topic-byod-and-the-consumerization-of-it/. Special issue of ZDNet online magazine.

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. 2011. Taming information-stealing smartphone applications (on android). Pages 93–107 of: Trust and trustworthy computing. Springer.

BIOGRAPHY:

Andrew A. Adams is Professor of Information Ethics and Deputy Director of the Centre for Business Information Ethics at Meiji University in Tokyo, Japan. He is currently chair of ACM SIGCAS (Special Interest Group on Computers and Society). He recently chaired USEC 13, the 2013 Workshop on Usable Security. He holds a PhD in Computer Science from the University of St Andrews and a Masters (LLM) in Advanced Legal Studies from the University of Reading. He has published papers on Privacy, Copyright, Digital Education, Computer Security, Physical Security, and Digital Identity. He is interested in too many things.