

Privacy invasions

New technology that can identify anyone anywhere challenges how we balance individuals' privacy against public goals

Karsten Weber

Nowhere has technological progress been as dramatic as in the field of information and communication technology (ICT). Citizens of the developed world now live in an environment in which access to electronic information and communication is nearly ubiquitous—and we rely heavily on being surrounded by this technology. In fact, it is so omnipresent that we only recognize our dependence on ICT when a network server or a communications system fails, leaving us cut off from cyberspace.

...computers, mobile telephones, personal digital assistants, music players and all other types of electronic gadgets are further shrinking in size, and we will soon wear them as we do clothes or jewellery...

The fields of biometrics and ICT aim to develop approaches that allow individuals to identify themselves and gain access to services without having to carry electronic gadgets or any physical means of identification, such as a credit card, driving licence or identity card. Although such technology, which relies on either implanted microchips or sophisticated and ubiquitous identification techniques, could make life easier, it also holds enormous challenges in regard to privacy infringement. Assuming that the necessary technology is universally disseminated, anyone could be recognized and identified anywhere on the basis of their personal characteristics or traits.

Steven Spielberg portrayed this technology in 2002 in the film *Minority Report*, in

which retinal scanners located in all public places allowed the immediate identification of anyone. Yet, this scenario is not purely science fiction: several European airports, including Amsterdam/Schiphol in The Netherlands and Frankfurt/Rhein-Main in Germany, have installed iris scanners to offer frequent flyers a fast-track check-in, bypassing the normal passport inspections. As a result of the PATRIOT Act, every non-American who enters the USA is now photographed and fingerprinted at the border control. In addition, new regulations from the US Department of Homeland Security demand that all non-US passports issued after 26 October 2006 must carry a microchip storing biometric information. In this article, I briefly describe current and forthcoming technologies, and discuss some of the ethical, social and political questions that they inevitably raise.

A closer look at existing ICT applications reveals that these devices have one common characteristic: although they are becoming progressively smaller in size, they have not yet invaded our bodies. Of course, their successive improvements have enhanced our abilities to communicate with each other and with machines, and to process information, but they nevertheless remain external devices. One consequence of this strict boundary between ICT and human anatomy is that human-computer interaction was, and still is, a good compromise between man and machine: although computer monitors, keyboards and the like are useful, they are by no means as easy to use as, say, our arms and legs. Yet current developments in ICT aim to overcome this boundary: computers, mobile

telephones, personal digital assistants, music players and all other types of electronic gadget are further shrinking in size, and we will soon wear them as we do clothes or jewellery—much like we now treat mobile telephones or iPods.

...implants could make human-computer interaction more 'natural'—eventually it could be like using our own limbs rather than an external tool

As ICT devices increasingly become an integral part of daily life, one important benefit is that human-computer interaction will become more intuitive. However, these devices still remain external to our bodies and must be recharged regularly, and we still have to hook them up to our personal computer if we want to update or change the information that they store. To close this gap, advanced research in ICT is about to make the final and logical step of integrating microelectronic devices into our bodies. Scholars such as Kevin Warwick at the University of Reading in the UK have already developed prototypes of ICT implants that are able to detect and analyse nerve signals, and use them to control other digital devices (Warwick, 2003; Warwick & Gasson, 2004). Such implants could make human-computer interaction more 'natural'—eventually it could be like using our own limbs rather than an external tool. Although there are surely some medical and other risks associated with implanting microchips into a human body and connecting them to the

nervous system, the potential advantages for the individual user might well outweigh such risks.

It is likely that the first generation of ICT implants will be used for personal identification. Microchips using radio-frequency identification (RFID) could be implanted, for example, under the skin of the elderly or individuals with mental disabilities to track their location and prevent them from becoming lost. An existing application is the identification of customers in a beach club: RFID chips that are implanted under the skin identify patrons everywhere they go, such as the bar or restaurant, so they do not have to carry a wallet or credit card (Jones, 2004).

All of the other applications of ICT implants that are currently under discussion are more or less science fiction. Artificial limbs or senses and the enhancement of our mental abilities are still far from realization. However, it is possible to identify some general characteristics that future implants will probably have: they will have long life in order to avoid regular replacement, which carries medical risks, and they will be able to communicate with other devices outside the body. Consequently, implants will need to be unambiguously identifiable, as is required by communication protocols. Implants will therefore identify themselves and, at the same time, the person who carries them.

Compared with existing implant technology, state-of-the-art biometric techniques are far more advanced and widely used. There are many more technologies, pilot programmes and real-life applications in place for biometrics than there are for ICT implants. In principle, biometrics uses one or several physiological or behavioural characteristics to identify a person. To do this, an initial registration of the individual's biometric characteristic is required, such as their fingerprint or iris pattern, to create "an individual biometric template" (Furnell & Clarke, 2005) that is then stored on a personal identity card or in a central database. The person can then be identified "by comparing an acquired sample against the template that is already held" (Furnell & Clarke, 2005).

Biometrics now uses a wide range of different technologies (Table 1; Clarke & Furnell, 2005; Furnell *et al.*, 2000), of which most laypeople will know at least one or two. Retinal scanning and voice verification have gained a large amount of

Table 1 | Physiological and behavioural characteristics used for biometrics

Method	Description
<i>Physiological</i>	
Face recognition	Extracts key measurements from a digital image of the user's face, and compares them with a stored 'faceprint'
Facial thermogram	Characterizes individuals by using varying temperatures emanating from different regions of the face
Fingerprint recognition	Assesses characteristic patterns of furrows and ridges on the fingertips by using optical, capacitive or thermal techniques to distinguish one person from another
Hand geometry	Measures the physical dimensions of the hand (for example, the span or the length of the fingers) when it is spread out on a flat surface
Iris scanning	Compares an image of the user's iris with a previously stored image
Retinal scanning	Scans the distinctive patterns on the retina
Vein checking	Assesses the characteristic vein patterns in the back of the hand by using infrared light
<i>Behavioural</i>	
Gait recognition	Characterizes individuals by the way in which they walk
Keystroke analysis	Monitors typing activity to determine characteristic rhythms; can be performed on the basis of known text (for example, in conjunction with a username and password) or keyboard inputs in general
Mouse dynamics	Monitors mouse-related activity, and attempts to characterize users on the basis of measures such as speed and accuracy
Signature analysis	Assesses a handwritten signature that is captured using a special pen and/or pad; static analysis simply assesses the resulting pattern, whereas dynamic systems also measure the pressure and speed of the signature
Voice verification	Compares a user's voice with a previously stored 'voiceprint'; can be performed on a text-dependent basis (that is, when speaking a known word or phrase) or text-independently

Adapted from Furnell & Clarke (2005).

publicity owing to their appearance in various blockbuster movies. Retinal scanning, for instance, featured in the James Bond film *Never Say Never Again*, made in 1983. At that time, the technology seemed to be highly sophisticated because it used lasers, and many people probably believed—and still do—that retinal scanning is secure. However, retinal scanning is often confused with iris scanning, which can be easily outwitted by such simple means as using a Polaroid photograph of an iris (Forte, 2003). Although voice verification and face recognition are regularly featured in movies, it is likely that the other technologies listed in Table 1 are not as widely known. Nevertheless, a considerable number of physiological and behavioural characteristics can be used to identify individuals.

Although ubiquitous computing is not a central theme of this article, I mention it briefly in the context of biometrics because it already massively reduces the privacy of information. As Barrera & Okai (1999) stressed: "To be in

cyberspace is to be recorded. Digital activities and objects are nothing but an ensemble of traces and records. ... Those digital footprints can be, by nature, reconstituted, recreated and saved indefinitely. Where a vast number of activities in traditional space are inherently non-traceable, cyberspace actions are the traces themselves."

There are many more technologies, pilot programmes and real-life applications in place for biometrics than there are for ICT implants

If a person leaves a physical space, for instance a park bench, it is extremely difficult, if not impossible, to track this action afterwards—that is, to prove that the individual spent half an hour there enjoying the sun. In principle, leaving a physical place means leaving it forever; by contrast, being in cyberspace means being there forever, because all of an individual's actions are stored immediately, and can be



© Royalty-Free/CORBIS

...in reality, it is difficult to draw a clear line between private and public situations, and between private and public goals

tracked and analysed. Furnishing real space with ICT will change the way in which we act as, in principle, every action will be traceable indefinitely. The advantages provided by ICT could therefore be countermanded by the infringements on our privacy: "... location services will often become repositories of potentially sensitive personal and corporate information. *Where you are and who you are with* are closely correlated with *what you are doing*. To leave this information unprotected for everybody to see is clearly undesirable" (Leonhardt & Magee, 1998).

The identification and authorization of users, and individually targeted marketing strategies, require the production, storage and analysis of personal information. Mobile ICT and ubiquitous computing environments cannot work without identifying and localizing users, because such systems provide location-specific and context-specific services. To react adequately to

customers' requests, service and content providers must gather data on their actions, behaviours and lifestyles. Biometrics can provide the means to identify and authorize users without requiring additional effort, and even without their consent. *Minority Report* demonstrated where this might lead—in one scene, retinal scanners identified pedestrians while big screens addressed them by name and showed individualized commercials. Notwithstanding such far-reaching scenarios, the idea of ubiquitous computing environments does not make sense without biometrics. In a way, if one talks about ubiquitous computing, one is also talking about biometrics.

When it comes to the use of ICT implants and biometrics to identify individuals anywhere and at any time, one important distinction must be made. These technologies can be applied for private and public goals, and can be used in private and public situations. Although it is possible to make a distinction between private and public on an analytical level, in reality, it is difficult to draw a clear line between private and public situations, and between private and public goals. Consider

a hypothetical scenario in which, in the near future, a company offers a combination of biometric techniques and ICT implants for personal protection—Blythe *et al* (2004), for instance, describe wearable computer technologies that would protect elderly people against disease and crime. In this scenario, implanted monitors would continuously transmit information about key body functions, such as blood pressure, temperature and heart rate, to a supervising surveillance system. In addition, the implant would send the exact geographic position of the person, as well as environmental data on the air temperature and humidity, noise levels and so forth (Prekop & Burnett, 2003). In the event of a critical condition, the surveillance system would issue an alert to security personnel. Many law-abiding citizens with serious medical conditions, such as chronic cardiovascular disease, might value this technology. Moreover, as it is a legitimate aim to protect oneself against injury or danger, it is not easy to argue against such an application.

...being in cyberspace means being there forever, because all of an individual's actions are stored immediately, and can be tracked and analysed

Even in this scenario, however, the technology not only benefits the person carrying the monitoring device but also affects other people. For instance, as the system monitors environmental conditions, it is also a mobile weather-surveillance device. Additionally, let us assume that it is combined with biometric technology to identify individuals who approach the carrier. Obviously, this would be a good measure to increase the level of protection against crime. Yet, at the same time, it would provide the means to inspect other individuals—in this way, a private monitoring device could become a public surveillance system. Even the existing low-technology option of RFIDs implanted under the skin of beach-club customers or elderly people, as described earlier, provides such a surveillance opportunity. The technology could be used to track individuals and monitor related characteristics, such as whether the person gathers in groups or prefers solitude. Even if the reader cannot imagine a use for such information, rest assured that marketing experts would find it highly valuable.

In effect, utilitarianism allows infringements of civil rights if they maximize the benefit for the majority...

How such technologies are applied ultimately depends on their social, economic and legal context. Regarding the social context, there are two main scenarios, which are often described as 'Big Brother' and the 'Panopticon' (Lyon, 2001; Patton, 2000). Roughly speaking, the term 'Big Brother' refers to a state that controls every aspect of its citizens' lives, as George Orwell described in his novel *Nineteen Eighty-four*. By contrast, the 'Panopticon' describes a society in which everyone is continuously controlling everyone else. Big Brother implies a totalitarian state and society, whereas a panoptic society would be entirely democratic. Although they are at the extreme ends of the spectrum, both cases raise important questions about whether and how it would be possible to guarantee civil rights. Of course, the Big Brother scenario implies that no civil rights are granted at all—particularly in the light of Orwell's book. Yet, even in a panoptic or entirely democratic society, one can ask whether and which civil rights can be protected, not least the right 'to be left alone'.

From a utilitarian point of view—and most current political debates are driven by utilitarian ideas—civil rights are not absolute constraints on state actions. If the majority of society considers the wide usage and application of biometric technology or ICT implants to be useful and beneficial, it will be difficult to argue against their application. In effect, utilitarianism allows infringements on civil rights if they maximize the benefit for the majority—we only have to look at the 'war on terrorism', which sanctions torture, wiretapping of citizens and imprisoning 'unlawful combatants' without proper judicial procedure. In contrast to such utilitarian positions, libertarians argue that civil rights

are absolute constraints on any such infringements by society at large.

During the Nazis' reign of terror, all concentration camp inmates were tattooed. Although it might sound polemic, it would be interesting to see whether the survivors of these camps would accept biometrics or ICT implants for personal identification. I guess the answer would be no. Of course, compared with current sophisticated ICT technology, tattooing is a primitive means of identification—although it worked perfectly well more than 60 years ago. Similarly to a tattoo, ICT implants are difficult to remove, and biometric characters cannot be removed without causing severe harm to the affected person—of course, you could remove your eyes, as in *Minority Report*, but that is not a real option. Being able to identify anyone at any time and anywhere might not be a great problem in a free and democratic society that is ruled by the law. Moreover, those who promote ICT implants and biometrics for identification purposes naturally do not support the use of these technologies for nefarious purposes. Unfortunately, as we have learned from history, societies and states can rapidly and completely change their character. Thus, we should not too easily or willingly allow the state, and its agencies, to employ the means and technology that would make possible the omnipresent control of its citizens.

ACKNOWLEDGMENTS

I would like to thank Ricarda Drüeke and Axel Schulz for their support, and for critical discussion of this paper. The article refers to the Mobile Internet Services and Privacy research project, which was funded by the German Federal Ministry of Education and Research.

REFERENCES

- Barrera MH, Okai JM (1999) Digital correspondence: recreating privacy paradigms. *Int J Commun Law Policy* 6. www.murdoch.edu.au/elaw
- Blythe MA, Wright PC, Monk AF (2004) Little brother: could and should wearable computing technologies be applied to reducing older

people's fear of crime? *Pers Ubiquitous Comput* 8: 402–415

- Clarke NL, Furnell SM (2005) Authentication of users on mobile telephones: a survey of attitudes and practices. *Comput Secur* 24: 519–527
- Forte D (2003) Biometrics: future abuses. *Comput Fraud Secur* 10: 12–14
- Furnell S, Clarke N (2005) Biometrics: no silver bullets. *Comput Fraud Secur* 8: 9–14
- Furnell SM, Dowland PS, Illingworth HM, Reynolds PL (2000) Authentication and supervision: a survey of user attitudes. *Comput Secur* 19: 529–539
- Jones V (2004) Baha Beach Club in Barcelona, Spain launches microchip implantation for VIP members (7 April). PrisonPlanet.com
- Leonhardt U, Magee J (1998) Security considerations for a distributed location service. *J Netw Syst Manage* 6: 51–70
- Lyon D (2001) Facing the future: seeking ethics for everyday surveillance. *Ethics Inform Technol* 3: 171–180
- Patton JW (2000) Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics Inform Technol* 2: 181–187
- Prekop P, Burnett M (2003) Activities, context and ubiquitous computing. *Comput Commun* 26: 1168–1176
- Warwick K (2003) Cyborg morals, cyborg values, cyborg ethics. *Ethics Inform Technol* 5: 131–137
- Warwick K, Gasson MN (2004) Practical interface experiments with implant technology. *Lect Notes Comput Sci* 3058: 7–16



Karsten Weber is a Professor of Philosophy at the University of Opole, Poland, and the Head of the Mobile Internet Services and Privacy project at the European University Viadrina in Frankfurt (Oder), Germany.
E-mail: kweber@euv-frankfurt-o.de

doi:10.1038/sj.embor.7400684