Privacy & Surveillance

Monitoring humans and monitoring human rights?

PEOPLE POWER FOR THE THIRD MILLENNIUM: TECHNOLOGY, DEMOCRACY AND HUMAN RIGHTS :: SYMPOSIUM SERIES 2008

Symposium Report

Edited by Kyle Scott

BioCentre

Edited by:

Kyle Scott
BioCentre, Project Administrator

BioCentre

51 Romney Street
London
SW1P 3RF

t: 020 7227 4706
e: info@bioethics.ac.uk
w: www.bioethics.ac.uk

Contents

Introduction

As we all become more familiar with the 'online' lifestyle matters of security become more important. When we do venture outside, the number of surveillance cameras monitoring our every move evokes questions over the emergence of a 'Big Brother' state.

The development of Radio-frequency identification Devices (RFIDs) offer endless opportunities for data collection but with no real boundaries to how far they could be used. Paying for the bus may be one thing, but monitoring our shopping preferences is something quite different. Like never before, issues of privacy and surveillance are very much at the forefront of people's minds.

In light of such developments, privacy laws must reflect the progress of technological developments and not lag behind. As digital surveillance increases, the nature of what surveillance entails also changes. The barriers to surveillance that once existed now seem to be rapidly diminishing as the prospect of tracking the precise movements and behaviour of every individual seem to be a very real prospect.

Who should decide what information is collected and monitored? Is privacy a thing of the past? Is the society that George Orwell depicted a model to aspire to or a case study to avoid at all cost?

Hosted by Lord Neill of Bladen in the House of Lords, BioCentre hosted an assessment of the issues surrounding privacy and surveillance informed by key academics and industry specialists within this field of study.

Lord Neill opened the symposium by setting the context for the event before proceeding to introduce Rachel Bell, Director of BioCentre, who introduced the first speaker of the afternoon, Professor Nigel Gilbert. Gilbert is professor of Sociology at the University of Surrey and chair of the Royal Academy of Engineering's group on Privacy and Surveillance. Further presentations were made by Mr. Simon Holloway, Practice leader for Bloor Research for RFID and a recognized European Authority on RFID and Professors Karen Yeung and Roger Brownsword of TELOS - the King's College London Centre for the study of Technology, Ethics and Law in Society.

A question and answer session concluded the afternoon which allowed the audience to engage with the speakers on various issues arising from each of the presentations. ■

What's wrong with a bit of high-tech surveillance? The social and individual benefits and costs of developments in surveillance technologies

Professor Nigel Gilbert

The afternoon's presentations began with Professor Nigel Gilbert's wide-ranging presentation on the benefits and costs of modern privacy and surveillance, entitled 'What's wrong with a bit of high-tech Surveillance? The social and individual benefits and costs of developments in surveillance technologies'. He began by commenting about how every day of the week there is an article in the newspaper about privacy and surveillance, and that although it was a positive thing that these issues were getting attention, the coverage of them was often oversimplified.

Prof. Gilbert offered the following definition of surveillance: to have information about one's movements and activities recorded; and to have that information processed in some way. This contrasts with article eight of the European Convention on human rights that states that privacy is a basic human right. He then outlined his intention to cover some of the technologies that are putting us under surveillance, to consider the consequences of those technologies for privacy and surveillance and to describe some ground rules for individuals, business and government.

The technologies that Prof. Gilbert described were divided into three categories: connection, disconnection and processing technologies. Connection technologies are technologies that move data around. The internet is one sort of connection technology that has become pervasive, and it allows you to move data from one computer to another. Mobile phones are another example, as long as your phone is on then its position is being constantly tracked so that your incoming calls can find you. Loyalty cards are also a form of connection technology because when you make a purchase in a shop, if you use a loyalty card then the data about what you have purchased is being stored on a computer.

Disconnection technologies control access; if we think of connection technologies as corridors then we can think of disconnection technologies as the locks on the doors that block your way. Examples of disconnection technologies would be ID cards that are used to determine whether you are permitted into a certain building or passwords that can only allow people who know them to access certain data. Prof. Gilbert also pointed out that there are many other disconnection technologies that are just beginning to come into widespread use such as biometric technology at the airport, and face recognition technology.

Processing technologies are technologies that allow us to search, merge or store data. Prof. Gilbert pointed out that keeping records is not new, and to demonstrate this he showed a picture of a vast storehouse of files from East Germany. However, what is new is that it is much easier to search a computer database, rather than a paper database. The way in which the computer has had dramatic effect is not in the storing of information, but in the processing of information. As well as looking up the data of an individual, this processing power can also be used to find a certain group of people such as males who live in South East England who are interested in buying a Bentley, which will be of interest to companies for advertising purposes, this is called profiling. Profiling can be used, not just for advertising, but also for detecting people who are likely to be criminals, terrorists or paedophiles. This can be done by compiling a list of common characteristics of the type of person that you are looking for, and this can be used to search a database for other matches. Profiling can be very good for businesses and it can also be useful for countering criminal activity, however, the categorising of people is never perfect, which means that some people are being picked out, who should not be. This group is called the false-positives.

Prof. Gilbert then went on to speak about the reasons for increased surveillance and threats to our privacy in this society. One of the reasons that he highlighted was increased personalisation. This means the tailoring of goods and services to the individual's needs, so for example, loyalty cards help businesses to tailor their offers to the individual by sending them coupons that match their shopping habits. This increased personalisation can become a possibility for surveillance because of the amount of information that is being collected about us. When a person purchases an Oyster Card in London they are encouraged to register that card so that if it is lost any money stored on it can be recovered. However, it can also be used to monitor your movements on public transport around London, and this information is then stored. Prof. Gilbert informed those present that the police make dozens of enquiries per month about the movements of individuals. Personalisation has the benefits of bringing us offers that fit our wants, but it also means increased surveillance. Prof. Gilbert said that the issue in these sorts of situations is often one of authorisation versus identification. Authorisation is when someone uses technology to prove that they are authorised to take a certain service or to make an act, whereas identification is when you are proving your identity to someone.

Another way that surveillance increases is through data sharing. Data sharing can often be very useful. A government report by Sir David Varney contained the story of a family, who after a family member had died in a road accident was required to report the death to government in 44 different ways. The conclusion was that this was because there was not enough data sharing between government departments and that if more data was being shared then this family would only have needed to report the death once. In some areas government is already involved in data sharing; the national DNA database contains genetic information about all convicted criminals and most suspects of more serious crimes. This database has been used by the police, through a process of data sharing, to convict criminals who otherwise would not have been caught. Another example of data sharing is Automatic Number Plate

Recognition (ANPR), where surveillance cameras read your number plate and then access the DVLA database to identify who owns the car.

Prof. Gilbert then spoke about the many things that we gain from this new surveillance technology. We gain more personalised services, and can make more savings on our shopping. We also get less paternalistic advice, that is, when companies make decisions about us that decision is no longer made by someone who has a personal relationship with us. Previously the decision may have been made by someone who was positively or negatively disposed towards us, whereas now it is being made by a computer on the basis of the data that it has about us. This can be seen in the case of bank loans; no longer is the bank manager who may or may not like us deciding whether we are eligible for a loan, instead it is a computer deciding on the basis of our credit history. Data sharing can be used for more efficient government or improved medical research. Increased surveillance can also bring about better conviction rates and increased child protection through profiling.

However, Prof. Gilbert went on to talk about the downsides of this new technology. Profiling has the tendency to undermine the idea that you are innocent until proven guilty. If you happen to fit the profile of a terrorist then you are likely to face problems when you try to take a flight, even though you may be entirely innocent. There is also the risk of creating a privacy divide between those who are well connected and have the ability and resources to control the data that is kept about them, and those who cannot. The most significant issue, Prof. Gilbert said, was the issue of trust. If the trust between government and people decreases then there is a tendency for government to increase surveillance, which in turn reduces the trust, and this can lead to a vicious circle where trust is continuing to decrease resulting in more and more surveillance. This can be seen to some extent in the example of Muslim communities in this country, where terrorist acts have led to a lack of trust, and this has led to increased surveillance and then a further lack of trust.

In conclusion, Prof. Gilbert said that there are gains and losses in this new technology, so finding a balance between these is vitally important and so is finding ways to mitigate the losses. We can improve safeguards, design with privacy in mind, and avoid giving away our privacy unnecessarily. These things can be achieved by using encryption more widely. Designers and businesses should be encouraged to think about whether what is needed in a certain situation is authorisation or identification, and authorisation should be used unless identification is essential. We can also make sure that businesses and government make risk assessments when personal data is involved. Prof. Gilbert then ended his talk by posing some questions for those present to think about: How much do you value your privacy?, Is surveillance a necessary evil?, Should government departments and agencies share information about its citizens?, Should there be higher penalties for losing data? ■

***Professor Nigel Gilbert** is the Director of the Centre for Research in Social Simulation at the University of Surrey as well as Director of the University's Institute of Advanced Studies and responsible for its development as a leading centre for intellectual interchange. Other professional activities include being the Chair of the Management Board of Sociological Research Online, Editor of the Journal of Artificial Societies and Social Simulation and a Member of Council of the Academy of Social Sciences.*

Making your life easier with RFID

Mr. Simon Holloway

Simon Holloway commenced his presentation by illustrating the use of RFID in everyday life, by asking those present how many of them had car keys which had a button activated device on the key fob. He explained this was an example of RFID technology which was becoming increasingly common in car manufacturing. He proceeded to talk about the Oyster travel card used within London as another example of RFID technology. The Oyster card uses RFID to transmit and exchange information at a low frequency each time the card is swiped on a bus or at a tube station. Likewise, new library cards being introduced across the London boroughs are using RFID as are many sports centres and other local amenities. As a passing comment, Holloway made reference to a local government initiative which is seeking to integrate all services provided by local authorities, such as libraries, sports facilities, council tax payment, by using smart card technology.

Proceeding to talk about the technology behind RFID, Holloway said that it was interesting to note that in many respects it was old technology. RFID originally came out of research carried out on radar during World War II as a means by which 'friendly' planes could be identified. By attaching RFID to British aeroplanes, a signature could be 'pinged' back to the control centre where the plane could be identified as being friendly. Therefore, the key principle of RFID involves radio waves which transmit at different frequencies, helping to identify an object, person or anything else that one wishes to identify. Holloway highlighted the fact that he saw the technology as being one of identification and not necessarily authorisation. Authorisation may become important after identification has taken place. An example of this could be found in the health service which Holloway would demonstrate later on in his presentation.

An important aspect which people very often think of when they consider RFID is the issue of tags and readers which form the hardware and visible component of the technology. Tags can come in all manner of different shapes and sizes which are then able to transmit at many different frequencies, allowing identification to take place from very small distances to anything up to 3 kilometres away. Holloway cited the example of the USA army and their use of RFID in Iraq. At US army depots, they have a series of containers which contain various supplies and provisions. Each container has a RFID tag attached to it which transmits a signal that corresponds with what it contains. A Hummer is then driven down the lanes of containers with a receiver onboard and depending on what is being looked for at the appropriate time, the necessary container can be found efficiently and swiftly. Holloway then contrasted this with the rather less efficient method employed by the British army of having to physically walk up and down the lanes of containers looking at the piece of paper which is stuck to each container! These examples help to illustrate the speed and accuracy of identification which RFID technology can bring to many different situations.

However, RFID technology is not simply a technology to be used on its own. In many respects, it is also an enabling technology allowing it to work with other systems and processes. In the previous presentation, Professor Gilbert had classified RFID as a 'disconnect technology', but Holloway stated that he would argue differently. He would argue that it is in fact all three forms of technology. First, it is a communication technology. 'Active' tags continually send out information effectively saying "I am here", whilst 'active/passive' tags lie dormant until activated either for a set of period of time or indefinitely. Secondly, RFID is a disconnect technology in exactly the way Professor Gilbert stated. It produces data which if not processed, has no meaning. This points to the third aspect of RFID which causes it to be an enabling technology; the data is translated giving it meaning and so enabling something to happen as a result.

Once the data has been translated, RFID middleware software is required in order to allow this enable to take place and be used in various applications. Examples of such applications include real time location systems (RTLS) and e-pedigree. RTLS can use Wi-Fi, GPS or RFID with the accuracy of these technologies being able to locate objects within 2cm of the actual object. But how could this be applied to everyday life? Holloway cited the example of portable x-ray machines in hospital. In emergency situations when a machine is urgently required, being able to locate where the nearest machine is could be life saving. On the other hand, e-pedigree concerns the USA pharmaceutical industry and is a particularly 'hot' issue in the state of California currently. This application of RFID helps to authorise the commodity of a drug and ensuring its validation and proof of manufacture.

Holloway then spoke briefly about his work with Bloor Research in this regard. He has recently been involved in helping to define what is involved in forming a piece of software to not only do the translation part of the process but also to control and integrate the process as a whole. The process does involve a combination of technologies in order to work effectively.

Examples of RFID usage

Holloway proceeded to talk about specific uses of RFID. He began with talking about health and safety with specific regard to the Norwegian ship building industry. In a Norwegian shipyard there can be anything up to 15 ships with a large number of workmen working on each one. The health and safety issues arise when some sort of emergency occurs and the status and location of every workman needs to be accounted for. An initial answer is to position a teller on each of the gangways to the ship who then records who comes off and who goes on to each ship. However, this would not be cost effective in terms of money and manpower. Instead, RFID technology has been used by placing a receiver in a gateway which is positioned over each of the gangways. Every workman wears a safety helmet and so a tag has been placed in the helmet. As each person walks through the gateway it checks and records who is on which ship and at what time. Despite the fact that it does introduce an aspect of monitoring the movement of people, the Norwegian unions have agreed to the technology as it is enhances the safety of personnel within the dock yards.

In a further example, Holloway spoke about the oil industry and BP's refineries in the USA. Following a particularly horrendous fire in 2005 at a refinery in Texas where three people lost their lives, health and safety has been seriously addressed. Sadly, the accident in 2005 revealed that of the three people who lost their lives, the relevant safety personnel did not know about two of them whilst the third should not have been in the area where the fire took place. Therefore, the challenge was to establish a system which would ensure people could access the parts of the refinery which they were required to along with the necessary equipment. In response, two decisions were taken. First, an identity card with a RFID chip inside was issued to everyone working within the refinery. The chip contains information on the individual in question, what they are allowed to do and where they allowed access. To access different areas, each person has to go through a security booth which has two doors. To open the first door requires the identity card to be inserted into a reader. If the person is allowed to access this area, the door will open allowing the person entry to the booth. Once they have entered the booth, the door will close behind them but the second door will remain shut. Above the booth is a sensor which can communicate with RFID tags placed in various pieces of equipment and clothing which the person should be wearing. Before the second door will open, allowing the person to access the area, checks can be carried out as to whether the person is wearing the necessary clothing - hard hat, flame retardant suit, boots etc. If any errors are found, a 'report' can be filed with the health and safety officer informing them that person x has tried to access area y unsuccessfully either because they are not authorised to do so or because they were not wearing the necessary protective suit. An additional advantage which arises from this RFID tracking system is that maintenance checks can also be carried out on equipment that is used around the refinery. Once again, the unions approved this system as it enhanced the health and safety of workers. Holloway acknowledged that in both cases, the systems introduced did constitute an aspect of surveillance and brought with them a slight invasion of privacy as people's movements could be tracked. However, he argued these issues were relatively small in comparison to the safety provisions the technology helped to introduce. The surveillance was for a specific purpose.

Oyster cards

Holloway went on to talk about the Oyster card in more detail. Two of the main reasons why the Oyster card was introduced was first, the issue of fraud – people were staying on longer than they should have been on their bus or tube routes without paying the appropriate fare and secondly, the ticket machines used on the tube network were approaching the time when they needed to be upgraded. Consequently, it was an appropriate time to make a change. The prevailing advantage that the Oyster card has over the paper ticket is that the process is far quicker and easier to use than having to insert a ticket into a machine and wait for the gate to open. The process of swiping in and out makes for a far easier and smooth process. On the issue of identification, Holloway made the point that this only becomes an issue if once you have a card you choose to register, in which case you become identifiable.

Healthcare

On the matter of healthcare, Holloway identified three key aspects which he would explore in detail. First, a problem encountered with those suffering from Alzheimer's is that it is difficult to ensure that they stay within the areas they are supposed to. Should they venture outside these safe areas, they could place themselves in unnecessary danger. An application of RFID in this instance is to place a tag in a bracelet that the Alzheimer sufferer then wears on their wrist. Within a controlled environment, the patient is allowed to move about as they so desire but when they approach a danger point, such as an exit door, someone can be informed and be called to assist the patient. What is more, the door can be locked and only opened if the tag in the bracelet is programmed to open it. This kind of system is being used to great effect in the USA but not currently within Europe or the UK. At this juncture, Holloway was quick to point out that very often Europe and the UK are well behind in the utilisation and application of RFID.

Another application of RFID in the context of helping the elderly is the call button system. This is emergency assistance system whereby the elderly person wears a small fob around their neck. The button is RFID enabled and when pressed immediately makes a call to a call centre which registers that the person is in some form of difficulty. Alongside the neck chain there is usually a phone in the building which does not need to be picked up and allows staff at the call centre to talk to the person who requires assistance. From personal experience with elderly relatives, Holloway acknowledged there were problems and difficulties with this kind of system. Nevertheless, the overall aim is positive and useful in so far as an aid, which helps elderly people to feel independent, is concerned.

Thirdly, the question of drug authentication was addressed. How can one prove that the drug being dispensed is the drug that it says it is? According to Holloway there can be many examples cited where drugs have been given to people and they turn out to be not what they say they are. This can happen in one of two ways; either the drugs are simply incorrectly dispensed or the drug has in fact been granted for sale to the third world and by some other means have come back into the first and second world markets. In such cases, the drug companies loose out financially but also the dosages could be wrong which therefore presents a threat to peoples' health.

In response, a number of initiatives have been introduced, including e-pedigree. One of the key problems with the drug and pharmaceutical industry is that a large number of different groups of people are involved and so implementing a process which can cope with this number of stakeholders is crucial. The legislation currently being addressed by the state of California addresses this issue from a legal perspective. Once again, Holloway noted that Europe is well behind on this particularly issue.

Concerning the Olympic Games, Holloway made the observation that RFIDs have been used at the games since they were held in Los Angeles in 1984 when the stocks of javelins were lost! The technology therefore came in useful in terms of keeping track of equipment. This year in Beijing, all athletes and those who are part of the Games' "family" such as officials, staff, coaches and support team members, will have RFID tags in order to gain entry and exit of buildings. In London for the 2012 Games, it is being proposed that no paper tickets will be produced but instead payment to attend the various events will be made through something akin to the Oyster card system. The card is swiped to gain entry to the various venues, checking the identity of the card holder, whether the correct payment has been made and whether or not the person is at the right venue. This card can be topped up with credit in much the same way as the Oyster card can be, thus removing the need for payment kiosks and the potential for money to be stolen. Moreover, the data generated from the system also has added benefits in so far as the co-ordination of the transport system is concerned. If the finishing time of every event is known along with the total number of people attending the event, the necessary adjustments can be made to the bus, tram, and tube etc timetables thus ensuring that the frequency of buses and trams can cope with the number of people wishing to use the transport system.

Holloway then showed and talked the audience through a video made in the USA showing what could be the shopping experience of the future. Using RFID technology in many different ways, including identifying groceries, stacking shelves, monitoring prices and the payment of groceries the whole task of shopping could be completely revolutionised and made easier. Holloway informed the audience that if they were to visit a Metro store in Germany then aspects of this experience were already being put into practice. He then proceeded to ask those present for their reactions to what they had seen. Did they consider it as any example of 'Big Brother' watching them or as a sign of convenience? If the response was 'mixed' – a combination of both – then Holloway suggested it was probably the best answer.

The real issues

To conclude his presentation, Holloway addressed what, in his view, were the real issues concerning RFID. He posited that it is not a case of dealing with something new but more a case of using something old in a new way. RFID has been around in excess of 60 years with the manufacturing industry using it for some time in order to track items on production lines. However, the big difference today is found in the fact that the tracking process is moving beyond the confines of one building to across organisations and buildings. Citing the example of Marks & Spencer, when one buys a suit from a Marks & Spencer store, it will have a RFID label on it which is used to track the good and to undertake a stock take. From personal experience, Holloway informed the audience that he knew that whilst previously the stock take in the Oxford Street store took one day, it now only takes one hour. Nevertheless, consideration needs to be given to how RFID tags are dealt with and removed from goods once they have been purchased.

With all Hewlett Packard products, RFIDs are attached to the packaging in order to track the goods pre-sale stage. However, no one else can read the tags once the product has left the store. Someone would need to have the necessary equipment in order and be very close to it in order to read the tag. Even then the information that can be read would hardly be of any use and not link the product with any specific individual.

This led Holloway to address the question of whether or not RFID presents a threat to privacy. In Holloway's opinion, it only presents a threat when an individual gives their consent to associate themselves with the data that can be obtained in order that a profile can be created. Whether or not the profile created is true or not is another matter. Over time it could happen that your movements and details in the home could be monitored which could prove advantageous as well as presenting a number of security issues.

Using the scenario of a broken washing machine, Holloway illustrated the benefits which could be experienced through RFID in the home. More often than not, when an engineer is called out to fix a broken washing machine, having looked over the machine and assessed what the problem is they often then find they have to go back to the depot to collect or order the necessary part. However, if a RFID tag were to be placed into each part of the washing machine during the manufacturing process, the fault could be diagnosed by the company by dialling into your washing machine, running a diagnostics programme, identifying the fault and then despatching an engineer with the appropriate replacement part. All this could be part of a "platinum service" which the customer could consent to when they purchase the machine. Holloway made the point that when the customer gives their consent to this kind of service, within clearly defined parameters, and agrees to 'open the door' to the technology, there are many benefits to be experienced. Following on from identifying these benefits, Holloway made the passing comment that some of these benefits could be lost should the proposed EU legislation on this technology be passed. Much of the legislation back tracks on RFID development.

In closing, Holloway concluded that the key is to get the balance right between invasion of privacy with the ready availability of information (what information we want to make available and when we want to) with the way in which we want to live our lives.

Mr. Simon Holloway *joined Bloor Research in 2007 as their Senior Analyst responsible for RFID, BPM and Manufacturing. He has written a number of white papers on RFID and 2 technical reports on the RFID Market as well as producing a number of product evaluations and articles. As of April 2008, Simon has become Practice Leader for RFID, BPM and Manufacturing. Simon Holloway is a recognized European Authority on RFID. He was the European Lead for Microsoft for RFID whilst being their Manufacturing Industry architect and is now a member of the Microsoft RFID Partner Advisory Council.*

Privacy, Fair Processing and Confidentiality in an Information Society

Professor Karen Yeung & Professor Roger Brownsword

The final presentation was a joint presentation by Professor Karen Yeung and Professor Roger Brownsword from the School of Law at King's College London. Prof. Yeung began by describing some news stories involving privacy and surveillance and Prof. Brownsword followed on from this by discussing the law surrounding issues of privacy and surveillance.

Prof. Yeung described three stories that had recently appeared in the news in order to highlight the contemporary issues that arise in our society to do with privacy, data processing and confidentiality. The first story concerned the launch of the National Staff Dismissal Register. The Register, which has been designed for those who are responsible for hiring staff, is an online database of employees who have been accused of theft or dishonesty in the workplace. Potential employers can access the database, which holds records for up to five years, when vetting job applicants. Employers will be able to search the database as long as they are signed up to the scheme that already boasts, among others, Harrods, Selfridges and Mothercare. Employers will be able to check whether job applicants have been dismissed or have resigned while under suspicion of allegations such as stealing, forgery, fraud, damaging company property or causing a loss to their employers or suppliers. Employees' details can be included on this register regardless of whether they have been convicted or even prosecuted. Trade Unions and Civil Liberties Groups have objected to this register because it leaves workers vunerable to the threat of false accusations.

The second part of Prof. Yeung's talk was a set of connected stories about a social phenomenon that has been referred to as 'e-venge'. Firstly she spoke about a social networking site based in the USA called Don'tDateHimGirl.com. This is also a database and it contains the details of over 46,000 men, most of which have been posted in anger by their former lovers to name and shame individuals and to warn others about getting romantically involved with them. Another example of e-venge is a man posting the contact details of his ex-girlfriend on an internet chatroom claiming that it is the contact details for a well known boy band. Not surprisingly, she received thousands of phonecalls at all hours of the day and night, and was forced to change her telephone number. Thirdly, is the example of an actress who made a video deriding her high-profile husband for a range of shortcomings including his sexual performance and posted it on YouTube. Such examples demonstrate why a company that has recently been set up, called Reputation Defender, is proving popular. This company promises to search the web, and remove anything that threatens to bring disgrace to you or your family, charging anywhere from $10 a month to $250,000 per engagement.

The third and final story from Prof. Yeung was superficially rather different. It concerns a young man, named Mr Wood, who was, in 2005, a press officer for an organisation called the Campaign Against the Arms Trade (CAAT) which opposed arms exports. In his capacity as a member of the organisation he attended the annual general meeting of an academic publisher that had recently purchased a company that organises arms fairs. Prior to the meeting CAAT had liaised with the police and it was agreed that two representatives would leaflet the share holders as they went into the meeting, and that no other demonstration would take place. Mr. Wood did not hand out any of the leaflets, but on his way out of the meeting stopped to talk to his colleagues who had been doing so. All the while, the police had been taking photos of members of the public who had been attending the meeting. It was then that they noticed that Mr Wood was in some way associated with CAAT and they started openly taking photos of him. They followed Mr Wood and his colleague to the nearest tube station, and stopped them both to ask them some questions. Mr Wood politely explained that he had not been engaged in anything unlawful and that he was simply going to proceed on his way to the tube station. The police continued to follow them into the tube station, taking photos of them, and this only stopped when the two reached the station platform. Mr Wood was not very happy that this had been happening even though he had not done anything unlawful. This led Mr Woods to bring a judicial review in the High Court challenging the legality of the taking of the photographs and compiling a file on him.

These stories do not reveal anything new or revolutionary Prof. Yeung claimed. They are merely new ways of doing what has already been going on. For example, the National Staff Dismissal Register can merely be seen as a way of speeding up the existing practice of checking applicants' references, rather than the old-fashioned method of phoning previous employers. The second set of stories can be seen as a modern manifestation of the old practice of kiss and tell as a way of seeking revenge on a past partner. The third story does not even involve any high technology at all; it is simply photography and surveillance of the old-fashioned kind. However, there is a link between these stories, because they all demonstrate the changing social practices and attitudes to privacy and surveillance. So, although it is true that the information found in the National Dismissal Register was always available before, including it in a database means that it is much more likely that it will be checked and also it is more likely to be treated as authoritative. Like-wise the widespread use of digital technology has greatly increased the rate at which 'you done me wrong' stories can be disseminated. For example, the YouTube video that was posted by the actress was viewed by more than half a million people in 6 days. Thirdly, the unease that is felt with the case of Mr Woods clearly implicates CCTV and all the other high-powered surveillance technology that is recording people who are going about their lawful business. At this point Prof. Yeung handed over to Prof. Brownsword for the conclusion to their presentation.

We live in an information society, and when we pause to think about whether we have concerns about this sort of society we usually say that we do; this is not a new message claimed Prof. Brownsword. However, he began by highlighting that what is new is that regulators have three resources with which to respond to these sorts of issues: privacy law, data protection law and confidentiality law. When people talk about privacy they often do not clearly distinguish between these three strands, yet for a regulatory system to function properly it is important that these concepts are clear and that they are relevant to our society.

Data protection law

Prof. Brownsword attempted to articulate what data protection law is for and why consent is a pivotal feature of that law. There are many criticisms of data protection law including that the law is out of touch with the technology that is currently available, and there are public interest objections particularly from the health profession who say that data protection is interfering with valid public health research. Prof. Brownsword agreed that many of these criticisms have some merit, but that the response to them should not be to weaken the requirement for consent. Consent, in order to be properly understood, should be anchored to rights. That is, that I, as a rights-holder, may sanction acts that would otherwise be a violation of my rights by giving my consent to those acts. It must also be observed that consent is of a strictly limited and rather specific nature because it merely precludes a certain wrong, but does not necessarily make the act right. The fact that a person authorises an act does not make it right, it just means that that person cannot complain about the act within the terms of the authorisation. Prof. Brownsword also pointed out that often consent plays too prominent a role in debates because it is thought that if anyone objects to what someone is doing then that person must get their consent, however, consent, properly understood, only requires that we get consent from anyone whose rights may be violated, not simply anyone who might be offended by the act.

To highlight some of these issues Prof. Brownsword used the example of Naomi Campbell being photographed by the press leaving a Narcotics Anonymous clinic in London. She did not want this photograph to be published, but this does not mean that the press need her consent to publish it unless it can be shown that by doing so they are violating some right of hers, and even then an act that goes against the interests of a rights holder can be justified if it can be shown that the act serves some higher right such as the freedom of expression. So a coherent data protection regime should major on the idea of individual rights and therefore consent should play an important role in such a regime. The existing regulation does focus on individual rights, however the language is rather out of date because it is based on a society with rather few and large computers and very visible data controllers; whereas the situation we have now is one where we have invisible data controllers and many more and varied data processors.

Informational privacy

Prof. Brownsword then went on to describe how the strands within data protection law could be disentangled. The challenge is to be able to articulate these strands in a way that is coherent and complementary, and also, that produces practical, workable solutions on the ground. The first of these strands is informational privacy. This is a concept that comes from the nineteenth century and it began as an idea that one has the right to one's private space, and this has developed into the idea that one has the right to control certain private information about ourselves. It is difficult to determine the scope of informational privacy. Privacy only protects a certain special class of information about oneself. For example, Prof. Brownsword pointed out that the information that he is a Professor of Law at King's College London is about him, but it is not private. Also, on his way to this symposium in the Houses of Parliament he was spotted by some of his students, so they went away knowing that he was in that area at that time, but this does not constitute an invasion of privacy because this is not special or sensitive information about him. It may be that what counts as private information is a matter of social convention, but it remains one of the challenges of privacy law to determine what it is that we want to protect under the guise of privacy.

Fair processing of data

The second strand is the right to the fair processing of data. Whereas privacy is a strand that predates the information age, the right to the fair processing of data arises because of the information age. In the information age data that has been collected by us is being processed routinely, so it becomes our interest to regulate, not just who has information about us, but also what they are doing with it. Prof. Brownsword said that he believed that there was often a conflation in the law of privacy and data protection. Data protection is not about protecting the data that a person holds as such, rather it is about protecting what a person can do with someone else's information (when that information is digitised and subject to mechanical processing).

Confidentiality

The third and final strand is confidentiality. Data is confidential if a person gives another person information that they otherwise would not legitimately have, and it is not permissible for a person to pass on to a third party any information held in confidence without consent. So, in the examples of modern day kiss and tell that Prof. Yeung described the strand that is being violated, if any, is that of a breach of confidence. However, it is difficult to determine what the agreement is between partners at the time they share information with one another.

The pressing question in this area is how do we understand the relation between these strands and how do we rank them. In discussion of rights it is often helpful to compare the relative importance of different rights, so for example, it seems clear that the right to life is much more important than the right to privacy, but it is much more difficult to give an order to privacy, data protection and confidentiality. When cases in this area get into the courts there is a tendency for the discussion to move from one strand to another. For example J K Rowling tried to block the publishing of a picture taken of her with her son on the grounds that this would infringe upon the privacy of her son; however, such a case confuses privacy with data protection. If a person is photographed in public it is not an invasion of privacy because this is not a private act, however, there may still be a data protection issue. Just because privacy is not being violated, it does not mean that there is not a data protection issue because the two strands are distinct.

Prof. Brownsword finished his presentation by highlighting some of the important questions that needed addressing, such as, how do we rank these three strands?, what are the values that we want protected by the law? And who are these rights being advanced against? These questions, and others, still remain unanswered and if we are to make progress in the area of privacy they must be addressed. ■

***Professor Karen Yeung** has been a Professor of Law at Kings' College London since September 2006, following twelve years at Oxford University. Since moving to the Centre for Technology, Ethics, Law and Society ('TELOS') at King's College London, she has focused her attention on new and emerging technologies. **Professor Roger Brownsword**, is Professor of Law at King's College London where he is Director of TELOS. He is also an Honorary Professor in Law at the University of Sheffield; and he is a member of the Nuffield Council on Bioethics.*