Green N, Smith S.

'A spy in your pocket'? Monitoring and Regulation in Mobile Technologies.

***Surveillance and Society* 2004, 1(4), 573-587.**

Surveillance & Society 1(4): 573-587
http://www.surveillance-and-society.org

'A Spy in your Pocket'? The Regulation of Mobile Data in the UK.

Nicola Green and Sean Smith[1]

Abstract

The growth of mobile digital communication devices has seen a corresponding growth in the data created by users in the course of their mobile communications. The ease with which such data - including sensitive time-dependent location information - can be collected and stored raises clear data protection and concerns. The value such data offers to both law enforcement agencies and the private sector has complicated regulatory responses to such data protection concerns. This has lead to the contradictory situation in which mobile data is used by the law enforcement agencies and the private sector to identify individual users, yet this same information is not considered to be 'personal data'.

Introduction

The development of hardware and software for information gathering in emerging, location-based mobile devices and services brings to light a sense of *uncertainty* surrounding the development of new mobile technologies. This uncertainty derives in part from the nature of the location-based technologies themselves – being, as they are, hybrids of already existing information and communications devices and networks. It also derives from the ambiguity surrounding how these technologies might be used on an everyday basis – it is, as yet, unclear how (or if) these technologies will become embedded in already existing practices of ICT use in daily life. The fragmentation of organizational responsibilities between telecommunications network operators and service and content provision in mobile technologies, the role of technology developers, market law experts and consumer advocates in standards setting and policy, the overlapping roles of different regulatory bodies, and some of the deep contradictions in ICT development and policy in the UK only adds to this sense of uncertainty.

We are currently engaged in a research project that explores these uncertainties as they come together in the interplay of production and consumption in mobile technologies. Our specific focus concerns the generation, ownership and control of personal and location-based information about individuals in mobile technologies, and understandings of privacy, risk and trust in the UK. Our rationale is that the rapid uptake and pervasiveness of mobile devices, and the

[1] Department of Sociology, University of Surrey, UK. website: http://risome.soc.surrey.ac.uk/

 ISSN: 1477-7487

ongoing development of location-based devices and services, presents a new paradigm for generating, organizing and sharing information about individuals and their lives. In this paper we will be examining one part of this new paradigm, namely the question of data protection in the mobile digital world.

Using data derived from interviews with regulators, mobile operators and privacy advocates, we argue that there is a fundamental contradiction between the collection, use and manipulation of the digital data created by mobile device use (both meaningful personal data and notionally a-signifying traffic data), and the regulatory and commercial stories about how and why this data collection takes place in the ways that it does. We argue that not only the *fact* of data processing and mining have social effects, but that these practices are themselves enabled or constrained by the stories or *operant fictions* about the meaning of data gathering that are told by state and commercial actors. Further, we shall argue that this contradiction is not a result of regulatory failure or an example of corporate malfeasance. Rather, this contradiction is inherent in the current understanding of data protection in the UK and EU, especially with respect to the state regulation of equally powerful commercial imperatives to maximize mobile markets and marketing. We argue that a new definition of 'personal data' is necessary if genuine protection to data subjects is to be available to citizens and consumers in the United Kingdom.

New Technologies and New Data Paradigms

The widespread development and distribution of mobile telecommunications technologies in recent years have further complicated already uncertain structures for the monitoring and regulation of personal data gathering activities in the western world. The data generated via mobile devices and their infrastructures add information about 'location' – or perhaps 'locatability' – into the intensifying streams of data potentially available for monitoring, storage, use and association by both individual and organisational social actors (Lyon, 1994, 2001).

These devices produce particularly powerful uncertainties for individuals, organizations and institutions because they are 'hybrid' in many senses – technical, institutional, social and interpersonal combinations of the familiar and the new. Technically, these devices or are hybrid in the sense that they combine existing and familiar technologies (and their attendant political economies) – both wired and wireless telecommunications systems and components, and information storage capacity and display – with newer and relatively unfamiliar technologies, including, for example, broadband digital streaming and satellite technologies, and the emerging political economies these imply. John Agar (2003) comments that new forms of global politics are to be found amongst the dust of a smashed mobile phone, and this globalisation of technologies applies equally to mobile infrastructural technologies and the data they generate. These familiar and new combinations of technology are clearly embedded in an expansion and interconnection of economies and markets that both make globalised mobile networks possible, and more deeply entrench the notions of 'mobility' and 'locatability' as commercially valuable pieces of information that have significant implications for mobilized global data flows.

Uncertainties also lie in the 'expanding mutability' (Norris and Armstrong, 1999) of the devices – the ways the technologies change over time, and/ or can be used for unintended purposes. The components and systems that comprise an operable mobile network, when coupled with the social and institutional structures required for their ongoing deployment and use, could potentially hold at least unintended consequences (if not intended expansions) in data gathering and storage activities. The technical hybridities entailed in new mobile systems require an equally hybrid set of institutional and organizational structures to produce, distribute and maintain them. Besides political economies, hybrid mobile technologies also imply hybrid forms of technical standards setting and regulatory mechanisms, necessary both for the systemic and global operability of mobile networks themselves, and for the organization and regulation of the data generated through them. Competing technical standards across the different technologies employed in mobile networks, and their associated social categorization as 'telecommunications' or 'information' technologies, can have significant implications for the policy initiatives and regulatory regimes that apply in uneven ways to emerging mobile systems, and the data they generate.

The public and private institutions that come to hold some significant relation to mobile technologies and data are therefore 'hybrid' in the sense that their activities and remits are multiple and overlapping with respect to both the use and regulation of the technology, and with the respect to the status and use of the information derived through them. Most importantly, mobile systems, and the institutions and organizations attached to them in various ways, create ambiguities in the associations between technical devices, systems and infrastructures, the data generated through them, the person associated with that data, and the regulatory regimes that purport to protect the privacy of that person and their information. Different regulatory, state and organizational actors treat mobile data as 'information' or 'communication' in different ways, have diverse remits, and therefore make different connections between devices, data and people. For example, the associations made between devices and people by mobile communication, depending on the communication, could be regulated under the auspices of three different regulatory bodies (The Office of Telecommunications [Oftel], the Independent Committee for the Supervision of Standards of Telephone Information Services [ICSTIS] or the Information Commissioner). The association between the *data* generated by mobile communications, and notions of 'personal privacy protection,' are by contrast mainly regulated through the various data protection legislations, therefore falling under the remit of the Information Commissioner.

These ambiguities in what the associations between devices, data and people actually *are*, are most obvious when we consider the notion of 'location-based information' and the case of its regulation. While mobile networks of communication are themselves multi-layered, with or without reference to increasingly sophisticated location-based technologies and data-gathering mechanisms, it is exactly in the case of location that a very particular kind of social and interpersonal hybridity occurs (which so far remain overlooked by the relevant regulatory mechanisms in the UK). The case of location data, through different interpretations, by different actors, of the association between technologies, data and persons, makes obvious the contradictions between the practices of data processing, and actors' narratives about data processing. 'Location data' involves the categorical association between devices, the information

generated through them, and the people to which they are attached. As our case studies below will demonstrate, the most fundamental contradiction we have identified in our research is the contradiction between the practice of data processing as if traffic data were connected to individual consumers (which gives the data its economic value), and the narrative of data processing that insists that traffic data is anonymous (which emerges from both regulatory and industry sources). 'Location data' therefore makes obvious the ways that these associations are being institutionally managed to favour not the protection of users' privacy and the protection of their data, but rather the operation of an increasingly unregulated (or voluntarily regulated) telecommunications industry in the UK.

Whereas 'mobile' and 'location-based' are terms that tend to be used interchangeably in discourse surrounding the data generated by mobile devices, 'location-based information' can be used in at least two senses. The first of these is that mobile-generated location data makes mobile data *'location specific.'* That is, the monitoring of data generated by mobiles makes the geographical location of a specific device the point of association between that device in space and a human being (data that is currently derived from mobile call traffic data). The second of these is that mobile-generated location data makes mobile data *'location-independent.'* That is, the monitoring of data generated by mobiles makes the *movement* of that device the point of association between that device in space and a human being (also currently derived from traffic data). The latter, implying movement, more strongly associates particular human bodies and the personal information attached to them to the location of the device itself.

The uncertainties and ambiguities in the associations between technologies, people and information create a situation in which different versions of technosocial 'hybridity' – the associations made between these elements – are actively constructed and mobilized in discourses surrounding changes to the current regulatory regimes that apply to mobile devices, networks, and the data that move through them. Most importantly, these constructions of hybridity are mobilised at the service of relatively powerful social actors in the state and corporate sectors. As we shall argue throughout this paper, the situation in which location-based information is assumed to refer to *location-specific data*, and to apply to a *device* rather than a person, a *contraction* of current regulatory practices in the protection of privacy and personal data occurs. Regulatory mechanisms on the protection of 'personal data' are assumed not to apply, and the regulatory schema that allows relative freedom of information-gathering activities, especially in the corporate sector, is routinely employed. By contrast, the assumption that location-based information is meant to refer to *location-independent mobile data*, and that the movement more strongly implies the connection of a human being to the device, encourages an *expansion* of current regulatory practices. This expansion is not, however, an expansion of relevant privacy protection regulations, but rather an expansion in the abilities of powerful actors (state actors in particular) to access the location data being generated by the mobile devices concerned.

In both these cases, the construction of particular sets of association between technologies, people and information serve to allow the expanded collection, monitoring and use of mobile and location-based information by a range of corporate and state agencies, at the expense of more robust and secure data protection and privacy legislation applying to mobiles in the UK. The

definition of what mobile-generated data is 'personal', how it is attached to an individual, and the significance of location in the links between person, data and privacy, are all questions that are implicated in how mobile data is treated in current regulatory regimes, and the impacts this has on the erosion of 'privacy.' We go on to consider below the specific ways in which data generated via mobiles is considered 'personal information' (or not) in current UK legislation, and the implications this has for notions of the 'personal' and the 'private' as they are constructed via state and corporate bodies to support mobile data-gathering activities.

Data protection in the UK

Data protection in the UK began with the Data Protection Act 1984 (DPA 84), which introduced rules governing the collection and processing of peoples' personal data by government and private sector bodies. It mandated such things as informed consent for data processing, in which consumers had to be notified in advance if their personal details were to be recorded and processed or sold to third parties; the provision of opt-out procedures, whereby consumers could elect not to have their personal data so processed; and the process for consumers to access their subject records. It was replaced by the enactment of the Data Protection Act 1998 (DPA 98) which came into force on 1 March 2000, with a first transitional period for data processing compliance implementation that ran until October 2001, and a second transitional period lasting until October 2007. This Act extended the 1984 provisions to include non-automated records, and reinforced a number of the data protection conventions in the DPA 84. Further secondary legislation such as the Telecommunications (Data Protection and Privacy) Regulations 1999, an annex of the DPA 98, was formulated to extend data protection rights to corporate bodies, and to limit the scope of unsolicited electronic marketing communications – specifically, email, fax and phone communications. These pieces of British legislation were largely in accord with a number of European Union directives, in particular Directive 97/66/EC of the European Parliament and of the Council, which sought to unify and harmonise European data protection legislation under the obligations of member states. The UK Information Commissioner draws upon European Directives such as this when issuing guidance to the interpretation of the British legislation.

The advent of mass market digital mobile telecommunications has brought a new urgency to the question of data protection, due the widespread circulation of what is known as traffic data – largely a-signifying transmission information necessary for digital mobile communications to take place, and the distinction with billing data, which constitutes 'personal data' covered by data protection regulations. In the UK, the Information Commissioner, following the European Commission's Telecommunications Directive (97/66/EC), has defined traffic data as data which:

> (a) are in respect of traffic handled by a telecommunications network provider or a telecommunications service provider;
> are processed to secure the connection of a call and held by the provider concerned

In the same advice, traffic data is said to constitute personal data when:

> the data subject is a subscriber to, or user of, any publicly available telecommunications service or, in the case of a corporate subscriber, would constitute such personal data if that subscriber were an individual.

Billing data, on the other hand, which includes such information as the subscriber's home address, the length, duration and place of their calls, and the time the call took place[2], is by definition personal data, and hence can only be processed by explicitly authorised bodies. Because all such information is carried in the traffic data of the call, the Information Commissioner has sought to clarify the distinction between traffic data and billing data, advising that:

> Because data processed to establish calls (known as traffic data) could potentially contain personal information which should therefore only be stored for limited purposes and retention periods, the Regulations provide for the protection of individual and corporate subscribers with regard to the processing of such data.
> Traffic data must be erased or dealt with in such a way that they cease to be personal data on the termination of the call in question.

In terms of data protection regulation in the UK therefore, the difference between billing data and traffic data boils down to whether or not the data is erased or anonymised at the end of the call. If the data is retained, without anonymising, then it qualifies as billing data, which as personal data is fully regulated by the data protection provisions of the UK and the EU, and its collection, collation and manipulation is restricted to registered data controllers who have gained the express informed consent of the data subjects to whom the data applies. If, on the other hand, the data is erased, or more significantly, retained but anonymised, then it qualifies as traffic data, and its collection and processing are not restricted by data protection or privacy provisions. In an interview with one of the UK's Deputy Data Commissioners, we were informed that anonymising calling data entails stripping it of the subscriber's name and address details, whilst retaining all other information, up to and including the content of the communication, the time, date, location and duration of the call, the phone numbers from which the call was made, and whence it was made.

---

[2] The Information Commissioner's advice is that: Billing data is defined as follows:

> (a) the number or other identification of the subscriber's station;
> (b) the subscriber's address and the type of the station;
> (c) the total number of units of use by reference to which the sum payable in respect of an accounting period is calculated;
> (d) the type, starting time and duration of calls and the volume of data transmissions in respect of which sums are payable by the subscriber and the numbers or other identification of the stations to which they were made;
> (e) the date of the provision of any service not falling within sub-paragraph (d);
> (f) other matters concerning payments including, in particular, advance payments, payments by instalments, reminders and disconnections.

Billing data may be any one or all of the above.

Corporate Surveillance

For the private sector the distinction between restricted billing data and fully archivable, cross-referencable traffic data is crucial. Consider, for example, what is known as the 'value chain' in SMS ('short message service' or text messaging) marketing on mobile phones. SMS marketing campaigns tend to be put together by a string of small companies as consultants to larger organizations working on everything from branding to mobile technology and data, interacting with larger actors such as network operators and client brands. A single SMS campaign involves the brand, its consultants and creatives who construct the user interaction, the application developer who creates the SMS interface, the application operator who runs the infrastructure that the SMS interface runs on, the application infrastructure provider who sends the actual text messages, and the network operator along whose network the text message is sent.

Traffic data moves along this value chain, from the network operator to the application providers and operators, all the way back to the brand. At each point in this chain, the traffic data is captured and archived by the companies involved, sufficiently comprehensively that data mining of this data can be listed on their books as a tangible asset. However, because the data has been anonymised – stripped of any subscriber name or address, but archivable by unique phone number (and in the case of opt-in SMS campaigns, also by six-digit postcode) – companies without billing relationships with the consumer are neither registered as data controllers, nor under data protection constraints as to their use of their traffic databases. As one interview respondent, an executive of one of the small companies that contribute to the mobile value chain, argued:

> We do not initiate SMS's ourselves, we don't send SMS's, we send them on behalf of people who ask us to send them, therefore we know nothing at all about the permissions underlying these SMS's. We know nothing about the level of consent people have given, and we don't hold the personal information in any way, except interestingly enough we have huge registers. In reality we keep every keep every message that gets sent. So I actually know every message that has been sent to every phone over the last two years.

Because the relationship between the mobile phone user and their phone number is arbitrary, is *indexical*, the respondent's company was under no obligation to either register as a data controller or to delete their traffic data logs, as the respondent described:

> However, the first thing that we did when we looked at the Data Protection laws was that we determined that all we ever knew about what was going on was associated with an index which is the mobile phone number. And all the personal privacy rules that I have ever seen relate to information that can be used to uniquely determine the individual, and I would strongly sustain that a mobile telephone number does not uniquely identify an individual.

A similar position is to be found within the Information Commissioner's office. When asked in an interview about the surveillance possibilities of location-based services, one of the Deputy

Information Commissioners (after describing location-based services as "not desperately exciting") said that:

> knowing precisely where a particular handset is would enable you to offer people ads… which is fine and dandy, but on the other hand, it implies a very close degree of potential surveillance of at least where a particular piece of equipment is. I must confess that rather puzzles me, because I often come across people saying that proves where somebody was, well it doesn't, because people use other handsets.

Here then is the paradox of data protection in the mobile digital world. The mobile phone is regarded by consumers, by industry and by regulatory bodies as a personal communication device in so far as it is assumed to be connected to a particular individual (hence the value of 'keeping every message that is sent' and the 'implication of a very close degree of potential surveillance). This ability to enable interaction with users is what makes mobile data economically valuable. At the same time, the mobile phone number as *index*, in the words of our industry respondent, is treated as a non-individuated, non-personal piece of information, on par with a bus ticket in terms of its privacy implications, for both regulators and industry. Strictly speaking, of course, this second view is correct – to paraphrase Baudrillard (1994), the map is not the territory. The representation of the user (in this case their traffic data, their data trace), is not the same thing as the user themselves. Hence, both industry representatives and governmental agencies act on the assumption that the appropriate regulatory regime to deploy is one that *contracts* the application of data protection legislation – the data protection legislation does not apply to traffic or locational data generated via mobile networks.

However, mobile phones are considerably more iconic than bus tickets, and not simply indexical – in the same way as personal addresses, whilst strictly speaking similarly indexical, are in practice iconic representations of individuals. Consider, for example, the practice of the Australian social security agency, Centrelink (a subsidiary agent delivering social security and student assistance services on behalf of the Department of Family and Community Services). This agency uses SMS communication to surveil benefit recipients, sending out warning text messages whenever recipients fail to attend work placements or job interviews[3], thus expressing confidence that even poor people on government support regard their phone as their personal property. Similarly, the executive of the mobile application company, who expressed a strong dislike of spam text messages – SMS sent without prior informed consent from the receiver of the SMS – stated that

> I take the view that the phonetop, that this medium is very, very powerful, and the phonetop is a very intimate place …[but] if people spam, what will happen is that it will piss people off very quickly. People's tolerance to spam is actually very low. So what will happen is that if spam, if unsolicited or irritating content,

[3] For a report on the new trial, as reported by the Australian Broadcasting Corporation, see: http://search.abc.net.au/search/cache.cgi?collection=abcall&doc=http/www.abc.net.au/news/australia/nsw/metnsw-9jun2002-2.htm

> unwelcome content, arrives on people's phones, they will very quickly refuse to acknowledge this channel any more, and we will lose access to them. And by the way, I'm not talking about the operators here, I'm saying people will have a psychological reaction of rejection and as that point we've lost the channel. So we can poison the wells if we're not careful.

Furthermore, one needs only to look at the recent report by the noted British anthropologist Sadie Plant (2002), entitled 'On the Mobile', to see evidence of the personalization of mobile phones, and the ways in which users have come to regard their phones as personal. Indeed, entire industries have developed, dedicated to enabling mobile phone users to personalize their phones with individual ringtones, fascias, logos and other accoutrements. In none of these cases is the mobile phone regarded as anything other than a deeply personal device, one in which there is a strong correlation between the device and the user, between the number and the subscriber. There are also indications of acceptance of the link between the device of the mobile phone and the person of the user in the British judicial system, as exemplified by the recent Damilola Taylor murder trial and Omagh bombing trials. In the Damilola Taylor murder trial, the mainstay of the defence argument for two accused relied on traffic data, which recorded calls made on a mobile phone owned by the accused – away from the scene, but at the same time, as the alleged murder took place. The defence attorney stated of the accused, that 'The bottom line is this: if they were using those phones at 16.47, they could not have committed these offences and the only verdict you can return is not guilty. That is hard, cold evidence'. In his critical ruling at the end of the trial, the judge stated that 'Whoever used those telephones could not have been involved in the death of Damilola Taylor,' clearly implying that the use of the device, and the person of the accused, were inextricably connected.[4] The traffic data indicated that the handset was somewhere else, and the prosecution could not prove that the handsets were separated from the users.

In the Omagh bombing case on the other hand, police investigating the Omagh bombing had identified likely suspects, and had traffic data from mobile phone use that placed suspects going to and from Omagh on the day of the bombing. The traffic data indicated that the handset was in a particular place, but no admissible evidence was presented to prove the suspects were with the handset. The police were therefore only able to gather one conviction, for conspiracy rather than for the bombing itself, because the phone that was used belonged to a person who all parties agreed was not present at the scene, having lent his phone to the probable bombers. In this case, *contra* the Information Commissioner's Office and the private sector's distinctions, the traffic data was deemed not to have associated itself simply with a number – which any person could be found to be using – but to a specific person, the subscriber to the service, against whom the conviction was gained.

---

[4] See: http://news.bbc.co.uk/hi/english/uk/england/newsid_1908000/1908648.stm, and: http://www.tiscali.co.uk/cgi-bin/news/newswire.cgi/news/telegraph/2002/04/12/news/77_.html&template=/news/telegraph/templates/main.html

Government Surveillance

Indeed, the distinction between traffic data and billing data is irrelevant for the public sector, as law enforcement agencies have, following the Regulation of Investigatory Powers Act 2000, and the Anti-Terrorism, Crime and Security Act 2001, gained full and unrestricted access to non-anonymised traffic data. Further, proposed amendments to the RIP Act from the British Government have attempted to extend these rights to all governmental and quasi-governmental agencies, although public outcry about these proposals caused them to be withdrawn.[5] Additionally, the recent Directive 2002/58/EC of the European Parliament, (the 'Directive on privacy and electronic communications') concerning amendments to the EU Directive on data protection[6] have codified these powers across the European Union. For the EU, Article 15(1) of this directive (derived from the European Convention on Human Rights, Article 8) now allows data protection and data privacy to be circumscribed by Member States when

> such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.[7]

Furthermore, Article 15(1) allows to Member States "adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in [Article 15(1)]". Recent binding opinions published by the Article 29 Data Protection Working Party – the EC body charged with interpreting the EC's data protection directive – have ruled that "the outer limits for these longer periods is the limitations period provided in national law"[8], which it notes for the UK is six years. It is worth noting that the Article 29 working party has not given security services completely unregulated access to personal data. In another recent opinion, on the legality of US Government plans to collect and process flight manifest information, the Article 29 working party has determined that while "the fight against terrorism is a necessary and valuable element of democratic societies", "respect for fundamental rights and freedoms of individuals including the right to privacy and data protection must be ensured" even whilst combating terrorism.[9]

---

[5] See the BBC news reports, ' "Massive abuse" of privacy feared', available at: http://news.bbc.co.uk/low/english/sci/tech/newsid_2038000/2038036.stm, and, ' "Snoop" plans raise privacy fears', at: http://news.bbc.co.uk/low/english/uk_politics/newsid_2037000/2037459.stm, for lists of government departments who were to be granted unrestricted access to users' traffic data.

[6] See the transcript at: http://www.gilc.org/as_voted_2nd_read.html, and: http://www3.europarl.eu.int/omk/omnsapir.so/calendar?APP=PDF&TYPE=PV2&FILE=p0020530EN.pdf&LANGUE=EN

[7] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002.

[8] Opinion 1/2003 on the Storage of Traffic Data for Billing Purposes http://www.europa.eu.int/comm/internal_market/privacy/workingroup_en.htm

[9] Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data. http://www.europa.eu.int/comm/internal_market/privacy/workingroup_en.htm

Nevertheless, the distinction between non-identifiable traffic data and personally identifiable billing data is largely irrelevant for agencies of the State such as law enforcement as far as questions of security and law and order are concerned. The effect of the RIP Act, reinforced by Directive 2002/58/EC, is to make traffic and billing data generated by a mobile telecommunication available on request to UK law enforcement bodies. Under the RIP Act, a senior officer (superintendent or inspector) is required to ask a telecommunications operator for traffic data (and each force has to nominate a single point of contact for processing the requisite paperwork). The Interception Commissioner may exercise oversight after the fact of traffic data requests, but the investigating officer in any case need only justify the request to a senior officer who is empowered to make that request.

By the end of 2002, the BBC was reporting that law enforcement bodies had made over 400,000 requests for traffic data from mobile network operators.[10] It is worth noting that in this article the BBC quotes unnamed police sources as being 'frustrated' that traffic data is not always available because data is typically only held – in line with the telecommunications companies' data protection obligations (under European Directive 2002/58/EC, and Article 29 Data Protection Working Party Opinion 1/2003 on the Storage of Traffic Data for Billing Purposes, with associated guidance from the UK's Information Commissioner) – for six months. The BBC report also cites a forensic engineer arguing that traffic data can link suspects to crimes, quoting him as saying "if a person makes a mobile call, potentially while involved in commission of a criminal act, it is possible to determine from [the traffic data] where the radio footprint would have been made." For this forensic engineer, and the unnamed police sources, there is no differentiation between the mobile as a device and the mobile user.

As if to drive the point home, one of the justifications for the Anti-Terrorism, Crime and Security Act, according to the Home Office, is

> Given the increased threat and changing nature of the terrorist networks intelligence on the movements and actions of terrorist is vital to ensuring the security of the UK. In particular communications data is an important investigative tool: allowing investigators for example to establish links between suspected conspirators (itemised bill) or to ascertain the whereabouts of a given person at a given time, thereby confirming or disproving an alibi (cell site analysis).[11]

Whilst billing data, by definition, allows for the identification of individual users, the use of cell site data – i.e. traffic data – to categorically establish an individual's, as distinct from a device's, location, would appear to contradict the claims of regulators and industry as to the non-personal character of traffic data. For the law enforcement community then, the narratives of the m-commerce (mobile commerce – business to consumer goods and service provision) industry and data protection regulators – that the mobile handset has no relationship to the user, and that the

[10] 'Phone firms "flooded" by crime checks'. *BBC Online*, 20 Dec 2002. Available at: http://news.bbc.co.uk/1/low/uk/2592707.stm

[11] See: http://www.homeoffice.gov.uk/oicd/antiterrorism/ria_antiterrorism.htm

collation and processing of pseudonymised traffic data has no data protection implications – appears to be inoperative.

This is *not* to claim that there is a direct link between a device and the user, as indeed the conviction recorded in the Omagh bombing case demonstrates, nor between the device and the subscriber, as the Damilola Taylor case implies. What we are arguing however, is that there is *some sort* of relationship between a device and its user, between traffic data, including location, and the subscriber. This link is not evidential, in the sense of being sufficiently verifiable to satisfy judicial rules of evidence, but is nevertheless reliable, in that traffic data points to a specific person, and by implication should qualify as 'personal data' as defined by successive iterations of the Data Protection Act. That it does *not* qualify as 'personal data' is due not to any qualitative difference between traffic and personal data, but to the *'operant fictions'* employed by both regulators and the mobile communication industry.

We are using the term 'operant fictions' here to argue that it is not only the social practices of collecting and processing mobile data that have important social effects and regulatory implications, but that the narratives that some significant social actors employ to describe and justify how mobile data is processed and collected also have significant social effects and regulatory implications. In these particular 'fictions', the collection of data identified only by phone number or by six digit postcode is defined as being non-personal, despite the fact that a mobile phone number points to a single subscriber and a six digit postcode identifies a group of three or four houses, both measures sufficiently precise to allow data mining techniques to precipitate personal data out of the supposedly non-personal data.

That the protection of business is seen by some actors as more sensitive than the protection of the consumer can be demonstrated by comparing the regulations concerning individual traffic data with those concerning the use of unsolicited fax marketing and unsolicited telephone calls, the Telecommunications (Data Protection and Privacy) Regulations 1999. These regulations sought to limit the scope of unsolicited fax marketing, especially to businesses, which previously operated outside the scope of the main Data Protection Act, requiring as it did neither the processing of personal data to facilitate nor the sending to a specific identifiable individual. As such, unsolicited fax marketing, whilst unwanted, was not illegal, given the dependence of the Data Protection Act on the processing of personal information of identifiable data subjects. In order to overcome these limitations, the Telecommunications (Data Protection and Privacy) Regulations defined distinctly non-personal corporate entities as individuals for the purposes of processing personal data (i.e. corporations became legal, as distinct from natural, 'persons' under law). It then subjected unsolicited fax and telephone marketing calls to 'persons' to regulations and constraints, notwithstanding the lack of personal data processing undertaken in order to make such calls. It was enough that such communication was unwelcome and intrusive, and tied up expensive corporate fax lines, for the Telecommunications (Data Protection and Privacy) Regulations to limit their unsolicited use. Similar protections could easily be extended to traffic data, to limit its collection, retention or manipulation except when specific informed consent was given by subscribers and users. As data protection for individuals currently stands, however, only the manipulation of traffic data is proscribed, and then only when it is associated with subscriber name or home address.

That the narrative of 'non-personal traffic data' is used strategically by different corporate and regulatory actors to maximize economic opportunities and contain consumer protection, is also demonstrated in the contradictory narratives offered by some agents of the state. As we have already seen, the Anti-Terrorism, Crime and Security Act 2001 and the Regulation of Investigatory Powers Act 2000, cited above, grants UK law enforcement agencies largely unregulated access to mobile subscribers' traffic data. As we have also seen, law enforcement agencies were not slow in making use of these powers. In addition, law enforcement often seeks the extension of personal information databases well beyond communications,[12] as data matching technologies have historically been the basis of investigative techniques amongst law enforcement – from confessions and line-ups to fingerprinting and wire-tapping.

From the perspective of law enforcement agencies then, the rise of digital technologies can be seen as a further opportunity to do this data matching. Indeed, this desire to extend 'traditional' state surveillance and investigative powers into new digital domains is the stated purpose behind the UK government's most recent plans to allow a wide range of non-law enforcement state authorities to have unregulated access to subscriber traffic and billing data. This agenda has been in public debate for over two years, despite political setbacks. In this case, the narrative is that the development of new investigative or surveillance powers is merely an administrative readjustment of currently existing capabilities. The trade-off in using this narrative for agencies concerned with government administration and law enforcement is that they must therefore treat a piece of information such as a mobile number as directly signifying a unique user of the device, such that processing of an individuals traffic data can be used to determine their communication and location at a particular time. That this is not a question of data protection is only due to the assumption amongst some state bodies that surveillance of traffic data is merely a codification of existing powers, translated into a new technological domain.

It is a truism to point out that new technologies allow new possibilities and undermine existing actualities – as Latour (1991, 1999) has argued, precisely what defines new technology is that it allows new programmes of action and transforms or disallows existing ones. And yet, the simple re-translation of existing practices to account for changed technological possibilities is at the heart of both state and private sector approaches to personal data in mobile communications in the UK. For different social agents and organizations in both the private sector and the state, mobile communications pose both a risk and an opportunity. The differing narratives adopted reflect a shared strategy of defending their existing practices whilst trying to take maximal advantage of the new possibilities on offer. For the private sector, consumer preference for mobile devices over older forms of communication, in particular landlines, threaten existing advertising and marketing models. However, mobile communications also offer the possibility of newer, even more effective direct marketing channels that may operate within the existing data protection regulations. The m-commerce sector circumvents the risk of the expansion of data protection powers by creating a narrative that formally disavows any connection between a

[12] See, for examples, 'Police seek DNA record of everyone', *The Guardian* 8 Sept 2003, available at: http://www.guardian.co.uk/guardianpolitics/story/0,3605,1037582,00.html; 'DNA database nears 2 million', *BBC Online* 25 June 2003, available at: http://news.bbc.co.uk/1/low/uk/3018504.stm; and 'Police DNA powers to be extended, *BBC Online* 27 March 2003, available at: http://news.bbc.co.uk/1/low/uk_politics/2890047.stm.

particular mobile number and a specific individual. For agencies of government such as law enforcement, citizen preference for mobile devices threaten existing models of internal security such as wiretapping and other location-dependent communications surveillance technologies. However, mobile communications also offer law enforcement agencies the possibility of newer, more effective investigative techniques through pervasive, location-independent, real-time surveillance – as long as there are no evidentiary problems with the relationship between the handset generating the traffic data and the individual who has subscribed to the service. State agencies circumvent this risk by regarding the mobile number as denotative of the individual subscriber – that is, by disavowing any *disconnection* between a particular mobile number and a specific individual.

Conclusions: Privacy Fictions

We have argued throughout this paper that there is a fundamental contradiction between the collection, use and manipulation of the digital data created by mobile device use, and the regulatory and commercial stories about how and why this data collection takes place in the ways that it does. Practices of data processing, and the categories of association between technologies, data and people that emerge from that processing, both have significant implications for the protection of personal data. What is defined as 'personal' and 'non-personal', what is defined as 'personal information' and what as 'data,' whether a 'device' and 'data' are monitored or a 'person,' are significant for how associations are made between people, devices and data, and therefore what data processing practices are allowed and proscribed. Crucially, it affects where data protection legislation is interpretively expanded, and where it interpretively contracts.

The most fundamental contradiction we have identified in our research with representatives of regulators, and with mobile industry actors, is the contradiction between the *practice* of data processing as if traffic data were connected to individual consumers (which gives the data its economic value), and the *narrative* of data processing that insists that traffic data is anonymous (which emerges from both regulatory and industry sources). It is with respect to some of the practices and meanings emerging from law enforcement agencies that the instability of this contradiction is underlined. The contradictory rulings of recent court cases, and the expansion of law enforcement powers under the Regulation of Investigatory Powers Act 2000, and the Anti-Terrorism, Crime and Security Acts 2001, collapse the distinction between traffic data and billing data, and in so doing negate the 'operant fiction' that mobile traffic data is anonymous and unconnected to individuals.

The contradictions between narratives and practices are not a result of regulatory failure or an example of corporate malpractice. Rather, they are inherent in the current understanding of data protection in the UK and EU, especially in the way that the regulation of data protection clashes with powerful commercial imperatives to maximize markets and marketing via mobile technologies.

We argue that a new definition of 'personal data' (which recognizes the personal nature of all mobile telecommunications data), and an activist regulator, are both necessary if genuine protection to data subjects in the UK is to take place. Bringing all operations concerning telecommunications data under the auspices of the Data Protection Act would be at least a first step towards these aims, and would not stop the profitable manipulation of either personal or non-personal data. It would, however, require all actors along the mobile value chain to register as data controllers, and might therefore also prompt the rationalization of the mobile marketing industry. This would also provide the transparency and the informed consent that all parties consider desirable.

Given the impending arrival of more comprehensive and extensive location-based services, it is no longer sufficient to maintain the narrative that traffic data is not personal data. What is required if, in the future, any form of mobile data subject protection is to be assured in the UK, is the recognition that the mobile phone number is not merely an index, but is also intensely, and irrevocably personal.

References

Agar, J. (2003) *Constant Touch: a global history of the mobile phone.* Cambridge: Icon Books.

Baudrillard, J. (1994) *Simulacra and Simulation.* Ann Arbor: University of Michigan Press.

Latour, B. (1991) Technology is Society Made Durable. In John Law (ed) *A Sociology of Monsters: Essays on Power and Domination*, London, Routledge

Latour, B. (1999) *Pandora's Hope: Essays on the Reality of Science Studies*, Cambridge MA: Harvard.

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society* Cambridge: Polity.

Lyon, D. (2001) *Surveillance Society: Monitoring everyday life* Buckingham: Open University Press.

Norris, C, & Armstrong, P. (1999) *The Maximum Surveillance Society: The Rise of CCTV* Oxford: Berg.

Plant, S. (2002) *On the Mobile* Report Commissioned for Motorola Corporation. http://www.motorola.com