

Prepaid Mobile Phones: the Anonymity Question

Gordon A. Gow
Department of Media and Communications
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
United Kingdom

tel: +44 (0)20 7955 7695
fax: +44 (0)20 7955 7248
email: g.gow@lse.ac.uk

This is a discussion paper to be presented at 'Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities.' Oxford Internet Institute, Oxford University. 8-10 September 2005.

Please do not quote from this paper without the author's permission.

Abstract

There is growing concern among law enforcement and national security organizations about the use of anonymous prepaid mobile phone service and its apparent role in aiding criminal and terrorist activities. As a result, a number of countries have implemented or are lobbying for a registration requirement for such service. Industry representatives and privacy rights advocates tend to oppose such regulatory measures, arguing that there is little practical value in attempting to register prepaid mobile devices. The issue raises important and relatively new questions about an entitlement to anonymity in the ownership of a networked communications device. The aim of this paper is to establish an analytical framework to support a wider debate on prepaid services, and specifically on whether there is a reasonable and appropriate case to make for the registration of prepaid mobile phones and other network access devices. The paper provides an overview of the issue as it was debated in a recent Canadian case and reports on preliminary findings from an international study funded by the Privacy Commissioner of Canada. The paper then formulates a number of debating points drawn from these findings, offering a tentative conclusion that from a privacy rights point of view there is a reasonable case against the registration of prepaid mobile phone service.

Keywords

Anonymity; telecommunications policy; prepaid mobile phones; privacy rights; Canada (case study)

6,000 words

Introduction

In March 2004, the New York Times reported that security authorities under operation 'Mont Blanc' had identified and detained members of an al-Qaeda logistical cell by tracking them to a Swiss prepaid mobile phone service. Swiss government officials cited the story to support a forthcoming prohibition on the sale of unregistered SIM cards within the country (Swissinfo, 2004). A month later, the terrorist bombing incident in Madrid was linked to an un-detonated package that reportedly contained a prepaid mobile phone wired to plastic explosive and hidden in a sports bag ("Al Qaeda reivindica los atentados en un vídeo hallado en Madrid," 2004; "The mystery of Madrid's prime suspect," 2004). The discovery reinforced unsubstantiated claims in the media that terrorists were using prepaid mobile phones to coordinate their activities. Following the London bombings in July 2005, similar media stories appeared in various sources, with the Guardian Unlimited website noting that 'Cellular phones tied to a regular account are easier to trace than calls made from cell phones using anonymous prepaid cards.'

If we are to believe the media reports then prepaid mobile phones have replaced the streetcorner payphone as the chosen method of those seeking anonymity in their communications, be they obscene callers, criminals, or international terrorists. Prepaid phone service is available for purchase in almost every country, often through third party retail outlets where customers might never be asked to produce identification as a condition of sale either for the phone itself or for the 'top-up' cards. For this reason, prepaid mobile phone service has captured the attention of law enforcement and national security organizations, some of whom would very much like to see regulatory measures put in place to eliminate these so-called anonymous prepaid mobile phones.

Is this a reasonable measure given the purported use of prepaid mobile phones by criminals and terrorists? Or, as some would have it, is registration a largely ineffective measure that will have a negative impact on the mobile phone operators and their customers? Is it an unnecessary, perhaps unlawful, invasion of personal privacy to require registration of a mobile phone? Moreover, what is the evidence base supporting this type of regulatory intervention and how is it justified in countries where it has been implemented? The answers to these questions remain uncertain, but it is my intent in this paper to begin to address these questions by presenting some early findings from a research study on the matter and to move beyond these findings to problematize the notion of anonymity, with a view to expanding the policy debate beyond what is currently evident in the media coverage.

The structure of the paper is as follows: I begin with a short background section, presenting key facts about prepaid phones and their importance to the mobile phone sector today and into the near future. Following this background, I then introduce the debate over mobile phone registration, presenting various perspectives by drawing on evidence gathered from a study that I am now conducting for the Privacy Commissioner of Canada. The paper then concludes by introducing Gary Marx's concept of 'identity traits' in order to problematize the relatively unexamined notion of anonymity and to present an alternative framing of the debate.

The Prepaid Market and Growth Prospects

Prepaid is a significant share of the global mobile phone market, although this varies widely from country to country. Table 1 shows the most recent figures for the OECD region, where prepaid service accounts for about 40 per cent of the mobile phone market. Topping the OECD is Mexico where over 90 of the mobile phone market is prepaid. South Korea sits at the bottom with no reported prepaid service in that country. In the EU, prepaid service makes up about 60 per cent of the total mobile phone market, with Portugal and Italy at the top at 80 percent and Finland at the bottom with about 3 per cent of customers using prepaid. In the United States, prepaid is only about 15 per cent of the market, whereas in Canada it sits at about 25 per cent of market share.

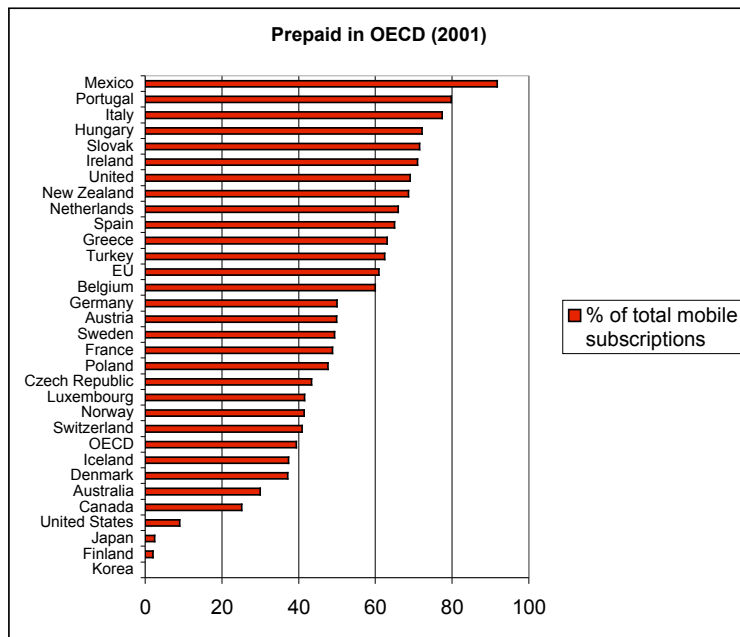


Table 1: Prepaid as a percentage of total mobile phone market in the OECD countries.
Source: OECD (2003) *Communication Outlook*.

Looking ahead, prepaid is anticipated to reach some 1.35-billion subscribers—59 per cent of the total global wireless market—by 2009 (Newman, 2004). As reported in Baskerville's *Global Mobile Prepaid Strategies and Forecasts* (2003):

- 50 per cent of the world's mobile phone customers now use prepaid, generating over one-quarter of the total revenues in the global market.
- Most markets continue to actively promote prepaid services, especially the largest and fastest growing markets in China and India.
- Between the end of 2002 and end of 2010, it is expected that 80 per cent of new customers will opt for prepaid services.
- The one billionth prepaid customer is forecasted to take up service in 2005.

- From 2005 and beyond, at least three-quarters of the total mobile phone market base will consist of prepaid users.
- By end of 2010 it is forecasted that there will be 1.5-billion prepaid mobile phone customers, generating over \$240-billion per year in revenue.

Table 2 indicates that in most parts of the world, prepaid growth is expected to be a primary driver of total customer growth in mobile phone service, with Western Europe being the only obvious exception.

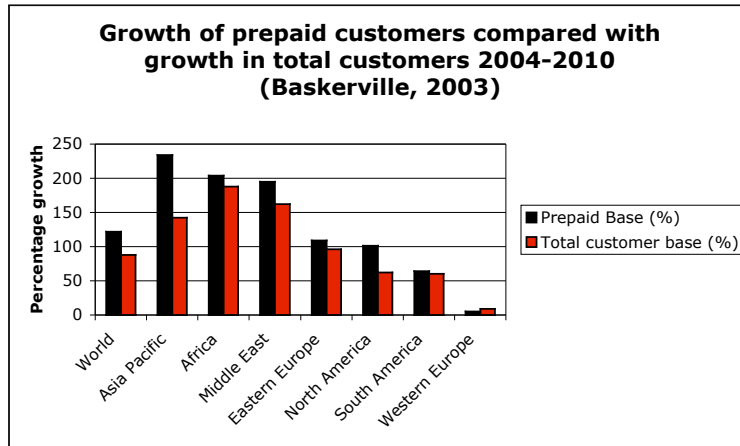


Table 2: Growth of prepaid customers compared with growth in total customer base for 2004-2010. Source: Baskerville, 2003

The Registration Debate

Debates about privacy rights and mobile phones have so far tended to focus on the issue of location privacy, partly in reaction to the advent of location-based services and new mobile positioning capabilities. For instance, a number of critical assessments have been made concerning location privacy and FCC’s wireless E9-1-1 mandate in the United States that requires mobile operators to provide real-time location data to emergency services when their customers dial 9-1-1 (Bennett and Regan, 2002). A central assumption made by these studies is that customer data has been collected at the point of sale and is held by the mobile operator in a database that is then accessible to law enforcement agencies or commercial location-based service providers. Privacy advocates concern themselves with the terms and conditions by which this customer information might be disclosed to third parties. I have referred to this elsewhere as the ‘first domain’ of location privacy research (Gow, 2005).

Alternatively, however, there is the case where a customer may choose to withhold personal data from the mobile operator because it is simply not needed to provide service, as in the case of prepaid (sometimes called ‘pay-as-you-go’) plans. In this case, the privacy question is about the terms and conditions by which an operator might be required by law *to collect and verify* personal information from their customers at either at the point of sale or before activating the service. This debate appears to be relatively

unexplored in the literature on information privacy, perhaps in part because prepaid mobile phone service is a new business model.¹ It raises an interesting question for privacy research: should there be an entitlement to anonymity in the ownership and use of a telephone? This question also touches upon a larger one if we extend it to include the ownership and use of other networked communication devices, such as desktop computers running VoIP applications, IP appliances that transmit and receive telematics data from a network, and even so-called 'smart cards' that provide stored value or facilitate other forms of network-based transactions. In other words, should there be an entitlement to anonymity in the ownership and use of *any* communication technology, much like there is an established entitlement to anonymous publication? The intent of this paper is not to delve into the bigger issue but to examine the question as it relates to mobile phones, and to derive some insights that might be then folded into the wider ethical-legal debate on the question.²

My first encounter with prepaid mobile phones and the anonymity question happened a few years ago when I was studying the Wireless E911 proceedings in Canada. The substance of these proceedings was the design and deployment of an 'enhanced' emergency service for mobile phones. Similar to the case in the United States, 'enhanced' or E911 means a system for the provision of real-time location information and caller line identification from a mobile phone subscriber to the emergency services operator handling a 9-1-1 dialed call.

In the course of the Canadian proceedings, one mobile operator revealed that a significant proportion of its customer base was on a prepaid plan and that it would not be feasible to provide the kind of detailed customer information that some emergency service organizations were seeking. The mobile operator stated in its remarks to the Canadian regulator that prepaid services are frequently offered through third party retailers who are not required to verify customer information and in some cases where prepaid phone packages are sold at convenience stores, retailers may not even collect customer information. The mobile operator argued that attempting to fulfil such an obligation for its prepaid segment would be onerous undertaking of little practical value and, moreover, that it might in fact violate provisions of Canada's privacy legislation:

... we submit that is entirely reasonable and legitimate for a customer to want to limit the disclosure of personal information when subscribing to a service, especially prepaid service where no monthly bill is issued and there is no apparent need for a subscriber address. ... Microcell [the mobile operator] submits that is by no means intuitively obvious to a reasonable member of the general public that a fixed address *must* be provided in order to receive mobile phone service. Resistance to providing fixed address information, therefore, is understandable, especially in light of the heightened awareness of privacy rights and concerns over the ability of organizations to protect personal data in the information age.' (Microcell Telecommunications Inc., 2001: 11)

From the perspective of this mobile operator, the collection of customer information in the form of home or business address is considered irrelevant to locating a mobile

¹ It is true that prepaid cards and payphones were introduced well before mobile operators entered the scene, but a key difference is that a mobile phone tends to be a personal communications device that is carried on the person and associated with that person's unique movements and calling patterns.

² For more about the wider legal and ethical debate concerning anonymity in a networked society, consult the anequity research project at <http://anequity.org/en3/index.html>

phone customer for public safety purposes, and possibly unlawful if gathered with respect to prepaid offerings.

In response to this position, certain emergency services organizations argued that customers *do not have a right to anonymity* with regard to any form of mobile phone service:

[Mobile operators] would have us believe they are now experts in privacy law, and their customer's [*sic*] have the right to be anonymous. How many wireline customers have this right, the answer is none. (Alberta E9-1-1 Advisory Association, 2002)

Prior to making this statement, the public safety agencies had previously put forward a recommendation that all new mobile phone customer activations be accompanied by two pieces of photo identification as a way of collecting and verifying their personal information for entry into the E9-1-1 system. The mobile operators industry, in opposition, characterized this as an action that would 'establish Canada as a wireless backwater compared to other countries' approach to consumer friendly communications,' suggesting further that such a requirement 'is unjustifiable and offensive to personal privacy' when it comes to prepaid services (Microcell Telecommunications Inc., 2002).

It was later when I discovered that the question of prepaid and anonymity had received attention in other countries. For instance, in 2002 Spain tabled a proposal with the EU to encourage member states to consider developing a set of harmonized regulatory requirements for identifying users of prepaid card technology. Representatives pointed to a 1995 European Council Resolution on lawful interception of telecommunications and claimed that 'the lack of regulation of anonymous prepaid telephone cards clashes with the need for law enforcement agencies to have access to telecommunications' (van Buuren, 2002). While no formal action on this proposal has yet been taken at the EU level, it is still the case that law enforcement organizations do appear deeply concerned about an apparent link between anonymous prepaid mobile phones and criminal and terrorist activities. Here is a selection of comments found in recent press reports, suggesting that prepaid registration might not be as 'backwater' as the Canadian mobile operator suggested:

... the Polish Ministry of Infrastructure introduced a new obligation for mandatory identification of buyers of pre-paid GSM-cards. The proposal is brought as an anti-terrorism measure.

-European Digital Rights, EDRI-gram (Dec. 2004)

'Removing the anonymous cards will be good for the fight against criminals,' said Police President Jiri Kolar, adding that the anonymity of callers often frustrated their investigations.

-Prague Post, 24 Feb 2005

The "community [now] has confidence that crime is not being facilitated through anonymous ... SIMs. Especially at risk are crimes like stalking, harassment, threats to interfere with witnesses. Also that that law enforcement has confidence in a database for emergency calls."

-Executive from Australia telecom industry

Opposed to such regulatory measures, however, are those who see little practical value in attempting to register prepaid mobile devices. This is a position characterized, or rather satirized, by John Lettice, writing in the UK online news source *The Register* in response to the Swiss case:

We at The Reg ... [have] had reports from all over Europe of how you could easily buy international-rated SIM modules for cash, no ID, no problem. We got the impression that most stores would probably call the police if you *tried* to force your details on them, and we were particularly impressed by the ease with which you could buy them in France, where they're actually supposed to take your details. You can even get round this by buying the French ones from a certain well-known UK chain; frankly, France Telecom's insistence on your filling in a form prior to buying one online sits as a splendid example of rectitude, isolated in a world of terror-friendly laxity. [emphasis in original]

He concludes the piece by referencing the Swiss requirement to register prepaid SIM cards for law enforcement purposes:

Once they've got records on all the cards in use, the security procedures will be simple. If they've caught an Al Qaeda terrorist and discovered he's using a Swiss SIM, they can look up the record of his address, then go and arrest him. No, we'll try that again. When they notice a suspicious pattern of usage, with calls being made from suspicious locations like Islamabad, Baghdad and Finsbury Park, they can look up the address he filled in and go and arrest him. No, we're not sure that works either... (Lettice, 2003)

Lettice, like some other privacy rights advocates and mobile operators, believes that registration is actually useless in those cases for which it is claimed it is most needed. While it may be true that prepaid mobile phones are a chosen communications device for criminals and terrorists, it is not necessarily true that registration of prepaid mobile phones will act as a deterrent to those who are serious about committing criminal or terrorist acts. In fact, the evidence, as suggested by anecdotal comments received by Lettice from his readers, seems to indicate that such a requirement is probably not enforceable in any reliable or consistent manner.

Nevertheless, the case of prepaid mobile services opens a wider debate as to an individual's entitlement to anonymity in the ownership and use of network access devices. Is there a legitimate case to make for the registration of mobile phones? Do these devices fall into a category similar to other technologies that require registration, such as automobiles or firearms? And if there is a legitimate case for regulatory controls on the sale of prepaid mobile phones should it logically extend to any form of network access technology, like a PC or internet appliance? Rather than attempt to provide a definitive answer to these questions, my intent with this paper is to establish the foundation on which a more extensive debate on the question might take place. Indeed, it is my view that the question is of considerable importance for setting precedent in the domain of electronic privacy rights and that a public debate must take place in those jurisdictions where regulatory measures are either under consideration or are now in force.

A Test of Reasonable Appropriateness

Perhaps the most obvious way to approach this debate is to consider it in light of current privacy legislation. In Canada, telecommunications services fall under federal

government jurisdiction where the *Personal Information Protection and Electronic Documents Act* (PIPED Act) applies. Section 5 of the PIPED Act establishes general terms and conditions for the protection of personal information and subsection 5.3 is most interesting for what it suggests about the collecting data from customers who might be purchasing or ‘topping-up’ a prepaid mobile phone:

An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. (Privacy Commissioner of Canada, 2000)

In other words, the collection of customer information by a mobile phone operator is subject to a test of reasonable appropriateness in Canada. On the one hand, the collection of personal information might be lawful under the terms of service between a telephone service provider and its customers, and indeed in the case of contract billing (so-called ‘postpaid’ accounts) the Privacy Commissioner of Canada has found this to be the case (Privacy Commissioner of Canada, 2001). On the other hand, however, section 5.3 might be cited to challenge the rightfulness of collecting subscriber list information for prepaid mobile phone customers.

To the best of my knowledge the Privacy Commissioner has not yet been asked to give opinion on such a challenge. However, in responding to a law enforcement proposal to require registration of prepaid phones in Canada, the Privacy Commissioner has made its position quite clear:

[Requiring customer identity verification] raises the spectre of convenience store clerks demanding and recording—and then transmitting—people’s sensitive personal information, such as driver’s license and credit card numbers, as a condition of purchasing pre-paid phones or phone cards. This would be a gross invasion of privacy. (Office of the Privacy Commissioner of Canada, 2002)

If considered against section 5.3 of the PIPED Act, this ‘gross invasion of privacy’ would stem from the fact that the collection of personal information is not needed to provide prepaid service and therefore it is neither reasonable nor appropriate to require its collection. Nonetheless, law enforcement might argue with equal effect that registration of prepaid mobile phones is indeed ‘reasonable’ and ‘appropriate’ as a measure to fight crime and prevent terrorism.

Given this predicament, a test of reasonable appropriateness might be settled in one of two ways. First, by producing empirical evidence to show that a program of registration has a deterrent effect on crime and terrorism. Such evidence might support registration as a ‘reasonable’ and ‘appropriate’. However, the Privacy Commissioner in Canada has stated previously that there is no empirical evidence to support such claims (Office of the Privacy Commissioner of Canada, 2002). My own investigation into this matter seems to confirm that there have yet been no published studies on the link between prepaid mobile phones and criminal or terrorist activities.³

On the other hand, it might not be necessary to produce such evidence and still present a politically acceptable case for adopting a registration policy for prepaid phones established on a principle of due diligence, or on a proportionality argument. During my

³ There is however a body of literature in criminology dealing with mobile phone theft.

initial investigation into the Swiss registration policy I discovered that this appears to be the view that carried the motion in the parliament, and against the recommendations of a panel that had been asked to report on the policy proposal. The view was that while most criminals are likely to use prepaid as a way of remaining anonymous, a registration program would effect only a small percentage of the population overall, making it a reasonable tradeoff in the name of public safety.⁴

Critics, however, might present an equally compelling argument that demonstrates that claims about registration are fallacious and that alternative methods of identifying telephone users are available that do not require a policy for prepaid. Such an argument might make a case that it is reasonable and appropriate for customers to withhold their personal information when purchasing a prepaid service and therefore support the claim to an entitlement to anonymity in the ownership and use of such devices in Canada and perhaps in other countries.

Giandomenico Majone has identified the persistent and often unexamined problem of logical fallacies, or *pitfalls* that sometime pervade policy analysis:

A pitfall is a conceptual error into which, because of its specious plausibility, people frequently and easily fall. It is the taking of a false logical path that may lead the unwary to absurd conclusions. A pitfall is for the practical arguments used in policy analysis what the logical fallacy is in deductive reasoning. In both cases, one has to be always on guard against hidden mistakes that can completely destroy to validity of a conclusion. (Majone, 1989, p.52)

Majone specifies, moreover, that a pitfall is not a simple error in procedure or in factual evidence, but instead stems from more fundamental flaw in the basic structure of an argument supporting a proposed solution or approach. In what follows, I will present a brief analysis to demonstrate a possible pitfall in the registration policy argument. To illustrate my analysis, I draw on the case of Australia where prepaid registration was introduced in 1997 and which remains the most accessible and detailed source of information I have found so far that describes a comprehensive policy of identity collection for telephone subscribers.

⁴ This observation remains to be confirmed and is presented here only as a preliminary finding. Here is the relevant passage from the meeting of the National Council from December 2002 (in original French): 'Après que la Chambre basse a elle aussi renoncé à inscrire dans le Code pénal une norme anti-terrorisme à caractère général, les débats ont porté principalement sur l'obligation d'enregistrer les téléphones portables à prépaiement, voulue par le Conseil des Etats. La majorité de la commission chargée de l'examen préalable du projet a proposé de biffer cette disposition, les porte-parole indiquant qu'il était douteux que les blanchisseurs d'argent sale, les revendeurs de drogue ou les terroristes présentent des papiers d'identité authentiques, sans parler de la possibilité d'utiliser des hommes de paille. Ils ont ajouté que l'enregistrement des identités entraînerait un travail disproportionné, compte tenu de ce que les criminels pourraient parfaitement recourir à des cartes à prépaiement étrangères. Une minorité emmenée par Doris Leuthard (C, AG) a cependant défendu la décision du Conseil des Etats, en faisant valoir que la quasi totalité des revendeurs de drogue utilisaient les cartes à prépaiement pour téléphoner, alors que l'enregistrement des identités ne concernerait qu'une petite partie de la population. Elle en a conclu que le travail que représenterait l'enregistrement serait raisonnable, surtout si l'on tient compte des avantages, notamment en termes de sécurité, qui résulteraient d'une telle obligation. Par 124 voix contre 7, le Conseil national a suivi la minorité de la commission, adoptant ainsi la voie tracée par le Conseil des États.' This record can be found on the Swiss Parliament website at: http://www.parlament.ch/afs/data/f/rb/f_rb_20020052.htm

Assumptions behind a Registration Policy

The Australian Communications Authority (ACA) has since 1997 has imposed regulatory controls on the sale and use of prepaid mobile phones, requiring all service providers to collect identification information from their customers prior to activation of the number (Australian Communications Authority, 1997, 2000). Service providers are required to collect the name and residential address (individual or corporate), the intended use of the service, and the total number of other activated prepaid mobile services supplied to that customer. This information is to be retained on file for as long as the service is activated.

The ACA regulation is predicated at least to some degree on the notion that anonymous telephone service presents a risk to society. The proceedings and various background documents that resulted in regulatory controls being introduced in Australia are not available to the public but the link to criminal and terrorist activities is evident in a 1997 press release announcing the measure, where it stated that ‘Law enforcement and national security agencies (had) also expressed concern about the implications of anonymous pre-paid SIM cards for law enforcement activities’ (Australian Communications Authority, 1997).

A closer look at the ACA regulations on prepaid services suggests that its registration policy is sustained by four key assumptions:

- Real-time or near real-time verification of personal identification is feasible in conjunction with the current prepaid market structure and with a variety of situations possible for SIM card activation.
- The collection of personal information at the point of sale or in conjunction with SIM card activation will lead to the creation of a reliable and accurate database of customers.
- The compilation of a database of customer information is more likely than not to assist law enforcement and national security efforts.
- A regulatory requirement to collect of personal information will have a deterrent effect on those customers who might otherwise consider using a prepaid mobile phone for criminal or terrorist activities.

Each of these claims may be problematic and without evidence they might be called into question regarding the practicality, costs, and social value of a registration requirement. First, it is not clear that real-time verification of personal identification is feasible within the current retail arrangements for prepaid mobile services. The ACA directive notwithstanding, Lettice’s comments in *The Register* (noted above) suggest that while registration requirements may be in force in some countries they are not necessarily enforced at the retail point of sale. Those with enough motivation and willing to spend the money could simply import a prepaid SIM from a country where no registration requirement is needed and assume the extra charges associated with roaming as part of the cost of remaining anonymous. Therefore, I would argue that enforceability is a problematic assumption. Another problem is the feasibility and cost of establishing a verification procedure for those retailers that would be required to comply with a

registration requirement. During the Wireless E911 proceedings, a Canadian mobile operator described the complications arising on this matter of verification:

Microcell [the mobile operator] ... wholesales its services to a series of non-affiliated resellers, each of which is 100% responsible for collecting and maintaining its own subscriber data. If the challenge of revamping activation systems to accommodate [customer] validation would be daunting and prohibitively expensive for a large 1.2 million subscriber operation like [Microcell], it would be nearly inconceivable for smaller non-affiliated resellers. A mandate to [provide] subscriber records ... would risk placing Microcell in the unacceptable position of having to enforce sanctions, possibly including termination of service, on resellers that fail to comply with a mandate whose rationale is dubious in the first place. (Microcell Telecommunications Inc., 2001)

The second claim that the collection of personal information at the point of sale or in conjunction with SIM card activation will lead to the creation of a reliable and accurate database of customers is also challenged by current practices among mobile phone customers. Evidence from sociological studies of mobile phone use indicate that sharing is a common practice among users and that resale and other forms of lending or incidents of loss or theft may challenge the ability (and willingness) of mobile operators to guarantee the accuracy of their customer records (Weilenmann and Larsson, 2001).⁵

The third and fourth claims are potentially undermined by findings in a report issued by the group Privacy International that conducted research to examine the link between identity cards and the prevention of terrorism. If regulatory controls on the sale of prepaid phones are to be effective they must set out a range of acceptable forms of identification (this is in fact an important feature of the ACA Determination). In fact, the entire scheme is premised *on the very existence of a reliable system for validating the identity of a prospective customer*. However, a recent report released by Privacy International did not find a significant strong correlation between the presence of national ID cards—arguably the most effective system for validating identity—and the prevention of terrorism. Such a finding suggests that a link between strong measures to validate identity and the deterrence of crime is problematic. The failure to find a strong relationship between the presence of strong identification schemes and reduced incidents of crime or terrorism also calls into question the link between registration and a deterrent in crime or terrorism and by implication challenges the reasonable appropriateness of a registration policy for prepaid phones.

Given the challenges to these four key assumptions it is not yet clear that a registration policy is in fact a ‘reasonable’ policy response to the perceived problem of anonymous prepaid service. In fact, the analysis tends to undermine the basic structure of the argument for a registration policy, at least in terms of a case based solely on supporting law enforcement and strengthening national security. The argument might be further undermined too, if we consider the conceptual fallacy that lies even more deeply

⁵ The Australian regulations are not clear on the matter of telephone sharing or resale.

embedded in the policy debate, particularly as the media has framed it by associating the term ‘anonymous’ with prepaid mobile phones.⁶

Is Anonymity Really Possible?

Sociologist Gary Marx has written that under the current conditions of rapid technological change and uncertainty surrounding the ethical aspects of anonymity, ‘at best we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point’ (Marx, 2001). The test of reasonable appropriateness may provide an orientation worthy of further pursuit in this regard, in part because it helps to problematize the concept of anonymity. Rather than establishing a universal perspective on an entitlement to anonymity, the test establishes a principle for debating and assessing the parameters of the concept of ‘anonymity’ when considered in specific circumstances.

Furthermore, the analytical pitfall of a registration policy for prepaid becomes more apparent when the very notion of ‘anonymity’ is subject to close scrutiny. Wallace, writing on the ethics of information technology, has considered the concept of anonymity and presents an interesting definition that models the concept on a continuum rather than portraying it as an absolute condition.

Anonymity has to do with the noncoordination or noncoordinability of the traits of a person in and through social ‘orders’, that is, in and through social relations and locations. ... Each person is a combination of interrelated traits; each trait is a position in a network of relations or equivalently, the location of the person in an order. Every person *is* a combination of traits, *is* located in multiple orders. (Wallace, 1999)

Wallace’s definition of anonymity describes a relationship between a person’s identity traits and the ability of another person to isolate and connect those traits into a coherent pattern. To take this idea further, we can look again to Gary Marx who has described seven forms of identity knowledge, which serve as basic categories of identity traits:

1. Legal name
2. Locatability
3. Traceable pseudonyms
4. Untraceable pseudonyms
5. Patterned behaviour
6. Social or physical attributes
7. Symbols of eligibility/non-eligibility

⁶ For instance, an article in the *Guardian Unlimited* (UK) used the phrase in reporting on the arrest of the London bombers in Rome, whom officials traced through his mobile phone. It is important to add too, that its mention in the article is actually quite incongruous with the substance of the piece overall. This kind of reporting on prepaid and terrorism is suggestive of the way this link between anonymity and prepaid is generally supported by media coverage. Here is the quote: ‘Cellular phones tied to a regular account are easier to trace than calls made from cell phones using anonymous prepaid cards.’ Dodds, Paisely. (2005, July 29). Last Suspects in Failed Bombings Nabbed. *Guardian Unlimited*. Retrieved July, 2005. Available <http://www.guardian.co.uk/worldlatest/story/0,1280,-5177074,00.html>

If we adopt Wallace's definition of anonymity and examine it with the various identity traits that might be linked to a prepaid mobile phone it becomes apparent that anonymity is difficult to achieve in practical terms. The following paragraphs describe the various identity traits and show how even when key bits information are missing, the remaining traits can be 'coordinated' to produce a reasonably coherent user profile for almost any prepaid mobile phone customer.

In an anonymous prepaid arrangement, the mobile phone telephone number serves as an 'opaque identifier' (Wallace, 1999) used to track calls made with the device and to debit the account accordingly. This opaque identifier provides a very limited possibility of true anonymity if we consider how it can be used as a key piece of information to coordinate other identity traits.

For example, consider a scenario in which a customer activates a prepaid account using cash rather than a credit card. Presumably this would provide maximum conditions for anonymity yet it eliminates only two or three of the seven possibilities for generating identity knowledge from the use of the telephone: legal name is not available; the mobile phone number as a 'pseudonym' traceable to an specific individual is removed; and, if the customer is able to avoid revealing other forms of personal information (e.g., age, sex, race, etc.) then it might eliminate social and physical attributes from being linked to the prepaid account. However, even an opaque identifier or 'untraceable pseudonym' such as a mobile phone number by itself still provides the possibility of generating at least three forms of identity knowledge.

First, the mobile phone may be used to make routine calls to a specific set of numbers, generating patterned behaviour traceable to other individuals, which may provide numerous clues as to the owner of the mobile phone particularly if the called numbers are known to or otherwise recognized by investigating authorities. Some of these called numbers could also reveal eligibility/non-eligibility criteria of the customer if they are associated with telephone banking or other password protected services. Furthermore, all mobile phones generate some form of location data even when on standby, meaning that it is possible to identify the general location of a mobile phone in real-time, as well as trace its movements over a span of time. The following table summarizes the various forms of identity knowledge available for an 'anonymous' prepaid mobile phone being used by a customer.

Identity Trait	Possible source
Legal name	None; name withheld by customer at point of sale; purchased mobile phone using cash
Locatability	A London-based mobile phone discovered through operator's call detail records (CDR) to now be roaming in Ottawa, Canada; person is on the move
Traceable pseudonym	None available (e.g., alias or business name)
Untraceable pseudonyms	Mobile telephone number with country code and city code
Patterned behaviour	Daily telephone call to a traceable number in London
Social/physical attributes	Potential CCTV footage of same person using the mobile phone in a certain place at a specific time of day (link to patterned behaviour and CDR)
Eligibility/non-eligibility	Phone used to call a telephone bank account (call detail records of mobile operator); DTMF tones reveal details as the person presses keys on the handset to access the account (this might require a real-time wiretap)

Table 3: Identity knowledge available for 'anonymous' prepaid mobile phones

This table is intended to show that there are various possibilities for generating identity knowledge about a prepaid mobile phone user without collecting their name and other personal information at the point of sale. By problematizing anonymity it calls into question the need for a registration policy and thereby challenges the reasonable appropriateness of such a measure provided other forms of identity knowledge are available to authorities. Prepaid mobile phones may present an inconvenience to legitimate requests for lawful access, public safety or commercial services, but they hardly presents the impenetrable wall of opacity presented by the media.⁷

Moving Forward with the Debate

Following the failed bombing attempts of 21/7 in London, authorities arrested one of the prime suspects in Italy after reportedly tracking his mobile phone as he moved across Europe. Once again, the media used this terrorist event to malign the prepaid mobile phone as aiding and abetting those responsible. One report, however, inadvertently illustrates that even in this case, it is not a single technology but a combination of technologies and particularly CCTV that were necessary to identify the suspect:

“That's definitely him. I'm really scared now,” Ana Christina Fernandes told a British policeman Thursday as he showed her a picture. A grainy CCTV (closed circuit television) photo showed a young man in tracksuit pants and a white tank top boarding the No. 220 bus. She identified Osman Hussain as her London neighbor.

A day later, the same man, who police say tried to set off one of four bombs on July 21, was captured by Italian police in Rome. He was betrayed by his mobile phone. Mr. Hussain was using a relative's cellphone as he traveled from Britain to France and Italy. By tracing the phone, Italian police pinpointed Hussain's location.

⁷ Yet another way to identify a prepaid mobile phone is through its IMEI number. This ‘International Mobile Equipment Identity’ code is a 15-digit serial number that is uniquely stamped on a mobile phone device irrespective of the SIM card used.

Identity knowledge is established by the coordination of different traits obtained from a range of technologies and circumstances. It is questionable whether a requirement for mobile operators to have collected personal information would have made a significant difference to the case, especially given the role of CCTV and eye-witness accounts in the initial identification and tracking of the suspect's movements.

The analysis I have presented in this paper indicates that anonymity may be impossible to achieve in practical terms and that a registration policy intended to eliminate 'anonymity' is probably unnecessary in practice. I would suggest that the policy debate might be more fruitfully directed toward wider concerns about the use and disclosure of communications traffic data from call detail recording (CDR) and various forms of circumstantial evidence, such as CCTV footage. Given these initial findings, privacy advocates and lawmakers might wish to resist a registration policy for prepaid mobile phones and other similar communications devices (e.g., WiFi cards) on the grounds that they are neither reasonable nor appropriate measures for the purported benefit claimed.

Beyond the regulatory domain of prepaid mobile phones, the question of an entitlement to anonymity should also prompt a wider theoretical debate about technology policy more generally. In particular, it may be time to consider the legal and ethical grounds on which some technologies are considered legitimate for registration (e.g., firearms, automobiles) and others are not, while thinking about how we might apply such reasoning to the regulation of a growing range of networked communications devices.

Works Cited

- Al Qaeda reivindica los atentados en un vídeo hallado en Madrid. (2004, March 14). *elmundo.es*. Retrieved Apr. 14, 2004. Available <http://www.elmundo.es/elmundo/2004/03/13/espana/1079203531.html>
- Alberta E9-1-1 Advisory Association. (2002, Jan. 28). CRTC 8669-C12-01/01 - Public Notice 2001-110 - Conditions of service for wireless competitive local exchange carriers and for 9-1-1 services offered by wireless service providers - Reply Comments - Phase II - 2001/01/28 - Alberta E9-1-1 Advisory Association. Available <http://www.crtc.gc.ca/PartVII/Eng/2001/8669/C12-01.htm>
- Australian Communications Authority. (1997, Dec. 22). Media Release No. 42 of 1997. ACA Makes Rule Applying to Pre-Paid Mobile Services. Retrieved Dec., 2003. Available http://aca.gov.au/aca-home/media-releases/media_enquiries/1997/index.htm
- Australian Communications Authority. (2000). Telecommunications (Service Provider -- Identity Check for Pre-paid Public Mobile Telecommunications Services) Determination 2000. Retrieved Feb., 2005. Available http://internet.aca.gov.au/acainterwr/aca_home/legislation/radcomm/determinations/telecom/telspid_1of04.pdf
- Bennett, Colin and Regan, Priscilla. (2002). What Happens When You Make a 911 Call? Privacy and the Regulation of Cellular Technology in the United States and Canada. Retrieved April, 2003. Available <http://webuvic.ca/polisci/bennett/research/CPSA2002.htm>.
- Gow, Gordon A. (2005). Information Privacy and Mobile Phones. *Convergence*, 11 (2), 75-87.
- Lettice, John. (2003, March 12). Swiss move to block al-Qaeda mobile phone supply. *The Register*. Retrieved Apr. 14, 2004. Available http://www.theregister.co.uk/2003/03/12/swiss_move_to_block_al/
- Majone, Giandomenico. (1989). *Evidence, Arguments, and Persuasion in the Policy Process*. New Haven: Yale University Press.

- Marx, Gary T. (2001). Identity and Anonymity: Some Conceptual Distinctions and Issues for Research. In J. R. Caplan and J. Torpey (Eds.), *Documenting Individual Identity*: Princeton University Press.
- Microcell Telecommunications Inc. (2001, Dec. 14). CRTC 8669-C12-01/01 - Public Notice 2001-110 - Conditions of service for wireless competitive local exchange carriers and for 9-1-1 services offered by wireless service providers - Comments - 2001/12/14 - Microcell Telecommunications Inc. Available <http://www.crtc.gc.ca/PartVII/Eng/2001/8669/C12-01.htm>
- The mystery of Madrid's prime suspect. (2004, March 22). *The Australian* (article from the *Sunday Times*). Retrieved Apr. 14, 2004. Available http://www.theaustralian.news.com.au/common/story_page/0,5744,9036002%255E2703,00.html
- Newman, Anthony. (2004, March 16). Prepaid phones to reach 1.35 billion users by 2009. *infoSync World*. Retrieved Apr. 13, 2004. Available <http://www.infosyncworld.com/system/print.php?id=4711>
- Office of the Privacy Commissioner of Canada. (2002, Nov. 25). Privacy Commissioner's reply comments regarding the "Lawful Access" proposals. Retrieved Apr. 19, 2004. Available http://www.privcom.gc.ca/media/le_021125_e.asp
- Privacy Commissioner of Canada. (2000). Personal Information Protection and Electronic Documents Act. Retrieved Dec. 12, 2003. Available http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp
- Privacy Commissioner of Canada. (2001, Nov. 8). PIPED Act Case Summary #24: Telephone company demands identification from new subscribers. *Commissioner's Findings*. Retrieved Dec. 11, 2003. Available http://www.privcom.gc.ca/cf-dc/cf-dc_011108_e.asp
- Swissinfo. (2004, March 4). Swiss phone cards help trace al-Qaeda. *swissinfo.org*. Retrieved Apr. 14, 2004. Available <http://www.swissinfo.org/sen/Swissinfo.html?siteSect=111&sid=4763869>
- van Buuren, Jelle. (2002, May 19). EU wants identification system for users of prepaid telephone cards. *Telepolis*. Retrieved Dec. 20, 2004. Available <http://www.heise.de/tp/r4/artikel/12/12574/1.html>
- Wallace, Kathleen. (1999). Anonymity. *Ethics and Information Technology*, 1, 23-35.
- Weilenmann, A. and Larsson, C. (2001). Local Use and Sharing of Mobile Phones. In B. Brown, N. Green and R. Harper (Eds.), *Wireless World: Social and Interactional Aspects of the Mobile Age*. London: Springer.