Bulletin of Science, Technology & Society

http://bst.sagepub.com

Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones

Gordon A. Gow and Jennifer Parisi

Bulletin of Science Technology Society 2008; 28; 60 originally published online Dec 27, 2007;
DOI: 10.1177/0270467607311487

The online version of this article can be found at:
http://bst.sagepub.com/cgi/content/abstract/28/1/60

Published by:

http://www.sagepublications.com

On behalf of:

National Association for Science, Technology & Society

Additional services and information for *Bulletin of Science, Technology & Society* can be found at:

Email Alerts: http://bst.sagepub.com/cgi/alerts

Subscriptions: http://bst.sagepub.com/subscriptions

Reprints: http://www.sagepub.com/journalsReprints.nav

Permissions: http://www.sagepub.com/journalsPermissions.nav

Citations (this article cites 3 articles hosted on the
SAGE Journals Online and HighWire Press platforms):
http://bst.sagepub.com/cgi/content/refs/28/1/60

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008

© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones

Gordon A. Gow
University of Alberta

Jennifer Parisi
Concordia University

In recent years there has been concern among law enforcement and national security organizations about the use of "anonymous" prepaid mobile phone service and its purported role in supporting criminal and terrorist activities. As a result, a number of countries have implemented registration requirements for such service. Privacy rights advocates oppose such regulatory measures, arguing that there is little practical value in attempting to register prepaid mobile devices, and the issue raises important questions about a citizen's entitlement to anonymity in the ownership of a networked communications device. This article provides an overview of the issue and presents findings drawn from a recent study on prepaid mobile phone regulation in the Organisation for Economic Co-operation and Development countries. The article concludes by suggesting that there are significant problems with the claim that mandatory registration of prepaid mobile phone service is a necessary or an effective regulatory course of action.

Keywords: *anonymity; telecommunications policy; prepaid mobile phones; privacy; OECD; public safety; terrorism*

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 subscriber identity module (SIM) cards within the country (Swissinfo, 2004). A month later, the terrorist bombing incident in Madrid was linked to an undetonated package that reportedly contained a prepaid mobile phone wired to plastic explosives and hidden in a sports bag ("Al Qaeda reivindica," 2004; "The Mystery," 2004). The Madrid discovery also reinforced other claims in the media that terrorists are now 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* Web site noting that "Cellular phones tied to a regular account are easier to trace than calls made from cell phones using anonymous prepaid cards" (Dodds, 2005).

If we were to believe the media reports, then prepaid mobile phones have become the method of choice for 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, with many pressing for strong regulatory measures that include mandatory identity verification and registration at the point of sale and/or activation of the phone.

There are those who would argue, however, that mandatory registration is a largely ineffective measure that will have a negative impact on the mobile phone operators and a large segment of the population that chooses prepaid service for any number of reasons, including lack of financial credit. Moreover,

Bulletin of Science, Technology & Society Vol. 28, No. 1, February 2008, 60-68
DOI: 10.1177/0270467607311487
Copyright © 2008 Sage Publications

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

it has been suggested that it is an unnecessary, even unlawful, invasion of personal privacy to implement regulatory measures to collect the identity information of those seeking to acquire a means of communication through a prepaid service. Such criticisms also beg the question as to the base of evidence supporting this type of regulatory intervention and how it is justified in countries where it has been implemented.

The aim of this article is to consider these critiques in light of findings from a recent study of prepaid mobile phone regulations in the Organisation for Economic Co-operation and Development (OECD) countries (Gow, 2006). The article begins 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. The article then introduces the debate and key findings related to mobile phone registration, concluding by introducing the concept of "identity traits" to suggest that the concept of anonymity itself needs to be reconsidered in order to establish reasonable and appropriate measures to balance privacy rights against legitimate public safety and security concerns.

The Market for Prepaid Mobile Phones

For some, it may come as a surprise to learn that prepaid service makes up a significant share of the global mobile phone market, even though the proportion will vary widely from country to country. Figure 1 shows recent figures for the OECD countries, where prepaid service accounts for about 40% of the mobile phone market. Topping the OECD is Mexico, where more than 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 ranges from more than 80% in Italy and Portugal to Finland at the bottom with about 2% of customers using prepaid. In the Americas, prepaid service is about 7% of the market in the United States and about a quarter in Canada, with Mexico topping the OECD with prepaid subscriptions composing 93% of the total market.

Forecasts made available a few years ago suggest that prepaid will continue to grow as a proportion of total market share to reach some 1.35 billion mobile phone subscribers—59% of the total global wireless market—by 2009 (Newman, 2004). It is also important to keep in mind that prepaid mobile phones are but one category within a much larger market of "stored value cards" that also include long-distance telephone service, gift cards, travel (public transit) cards, and payroll cards. A 2004 report issued by the

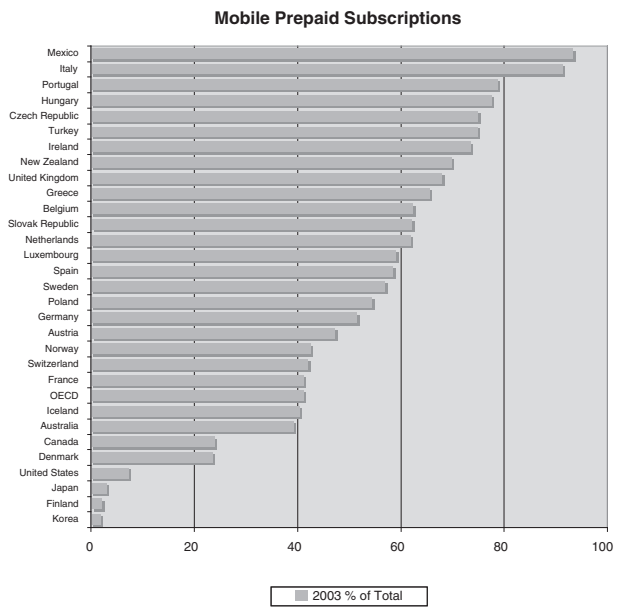

Figure 1. Prepaid as a Percentage of Total Mobile Phone Market in the Organisation for Economic Co-operation and Development (OECD) Countries.
Source: OECD (2005)

Federal Reserve Bank of Philadelphia suggests that the overall market for stored value cards will increase in the future:

> Many merchants, card associations, and issuers argue that the prepaid card market is on the verge of a major expansion, and some are already investing heavily in developing new prepaid products. Mastercard, for example, estimates that prepaid cards have the potential to move $0.5 trillion in traditional consumer payments and $1.5 trillion in other types of payments (e.g., business to business, government to consumer, etc.). (Furletti, 2004, p. 9)

Wider efforts by governments to control anonymous transactions by regulating this growing prepaid card market could lead to proposals for merchants to collect and register customer information for other types of services besides prepaid mobile phones, to prevent fraud or to address other legal concerns related to "anonymous" users.

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

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

services and new mobile positioning capabilities. For instance, a number of critical assessments have been made concerning location privacy and Federal Communication Commission'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 & 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. This has been referred to elsewhere as the "first domain" of information privacy research (Gow, 2005).

Alternatively, however, there is another domain of privacy research that involves cases where a customer may choose to withhold personal data from a mobile phone service provider because it is simply not needed to provide the service, as in the case of prepaid (also called "pay-as-you-go") plans. In this case, the key privacy question is about the terms and conditions by which an operator might be required by law *to collect and verify* personal information from its 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 relatively new business model.[1] The debate is important, however, in part because it raises an interesting question for privacy research: Should there be an entitlement to anonymity in the ownership and use of a prepaid mobile phone?

In 2002, for example, 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). Although 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. The media and industry have also reported on similar measures considered elsewhere, highlighting the link between prepaid phones and crime:

> 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, 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. (Bouc, 2005)

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 U.K. online news source *The Register* in response to the Swisscom 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. (Lettice, 2003)

He then 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)

Like other privacy rights advocates and many mobile phone providers, Lettice (2003) claims that mandatory registration is ineffectual in those cases for which it is claimed it is most needed. Although it

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

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—at least that which is available to the public—is slim on this question despite the fact that anecdotal comments, like those received by Lettice from his readers, seem to indicate that mandatory registration is probably not enforceable in any reliable or consistent manner in many cases.

By extension, these views might also apply to the ownership and use of other networked communication devices, such as desktop computers running Voice over Internet Protocol (VoIP) applications, stand-alone IP appliances that transmit and receive data from a network, and even the "smart cards" that provide stored value or facilitate other forms of network-based transactions. In other words, prepaid mobile phones suggest a broader set of questions about the ownership and use of *any* networked communications technology—questions that form a wider research agenda concerning anonymity, ethics, and technology law (e.g., Kerr, 2007).

A Test of Reasonable Appropriateness

One way to frame this debate is to consider it in light of current privacy legislation. In Canada, for example, 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 collecting data from customers who might be purchasing 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.

The Privacy Commissioner has not yet been asked to give an opinion on such a challenge. However, in responding to a law enforcement proposal to require registration of prepaid phones in Canada, the Privacy Commissioner 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 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 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), and a recent study conducted by the author among OECD countries into this matter confirms this statement (Gow, 2006).

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. Data gathered as part of the study among OECD countries indicated that a mandatory registration regime was introduced in Switzerland against the recommendations of a panel that had been asked to report on the policy proposal. The view of supporters was that although most criminals are likely to use prepaid as a way of remaining anonymous, a registration program would affect only a small percentage of the population overall,

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

making it a reasonable trade-off in the name of public safety (Government of Switzerland, 2003).

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.

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 the 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 flaws in the basic structure of an argument supporting a proposed solution or approach. In what follows, findings from a case study of the mandatory registration regime in Australia will be used to demonstrate a possible pitfall in the policy argument.

Assumptions Behind a Mandatory Registration Regime

In 2006 the Australian Communications and Media Authority (ACMA) renewed its commitment to a mandatory registration regime by holding a public consultation process with the aim of closing loopholes in its identity verification procedure (ACMA, 2005, 2006). The regime dates back to 1997, when Australia first 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 Australian 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 (reiterated again in the 2006 consultation) where it first 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 Australian 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 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 is problematic to some extent and, without a base of empirical evidence available for analysis, they might each be called into question regarding the practicality, cost, 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 current directive notwithstanding, Lettice's comments in *The Register* (2003) suggest that although 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 willingness 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

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

cost of remaining anonymous. Therefore, 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. This problem is in fact the primary reason for the ACMA's recent consultation on prepaid registration. In Canada, the problem was highlighted during regulatory hearings to examine challenges of registering prepaid phones for 9-1-1 emergency service. A Canadian mobile phone provider described the complications related to identity collection and 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 & Larsson, 2001).[2]

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 original regulation). In fact, the entire scheme is premised on the very existence of a reliable system for validating the identity of a prospective customer (Lyon & Stalder, 2003).

However, a 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 (Privacy International, 2004). 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 embedded in the policy debate, particularly as the media has framed it by associating the term "anonymous" with prepaid mobile phones.[3]

What is "Anonymity" Anyway?

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 principle of "reasonable and appropriate" measures may provide an orientation worthy of further pursuit in this regard, in part because it suggests that there are conditions when mandatory registration is unreasonable. Rather than establishing a one-size-fits-all perspective on the entitlement to anonymity, the idea establishes a higher-order principle for debating and assessing the parameters of the concept of "anonymity" itself as contextually bound.

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.

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

> 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 (1999) 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 (1999), who has described seven forms of identity knowledge, which serve as basic categories of identity traits:

Legal name
Locatability
Traceable pseudonyms
Untraceable pseudonyms
Patterned behavior
Social or physical attributes
Symbols of eligibility/noneligibility

If we adopt Wallace's (1999) 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 of 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 a 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.

Table 1. Identity Knowledge Available for "Anonymous" Prepaid Mobile Phones

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 behavior	Daily telephone call to a traceable number in London
Social/physical attributes	Potential closed circuit television (CCTV) footage of same person using the mobile phone in a certain place at a specific time of day (link to patterned behavior and CDR)
Eligibility/ noneligibility	Phone used to call a telephone bank account (call detail records of mobile operator); dual-tone multi-frequency tones reveal details as the person presses keys on the handset to access the account (this might require a real-time wiretap)

First, the mobile phone may be used to make routine calls to a specific set of numbers, generating patterned behavior 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/noneligibility 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. Table 1 summarizes the various forms of identity knowledge available for an otherwise "anonymous" prepaid mobile phone being used by a customer.

Table 1 is intended to show that there are various possibilities for generating identity knowledge about a prepaid mobile phone user without collecting their

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

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 present the impenetrable wall of opacity presented by the media and some in government.[4]

Moving Forward With the Debate

Following the failed bombing attempts of July 21, 2005, 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 travelled from Britain to France and Italy. By tracing the phone, Italian police pinpointed Hussain's location. (Thorne, 2005)

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 phone providers to have collected personal information would have made a significant difference to the case, especially given the role of CCTV and eyewitness accounts in the initial identification and tracking of the suspect's movements.

The analysis presented in this article indicates that anonymity may be impossible to achieve in practical terms and that a registration policy intended to eliminate "anonymous users" may very well impose unreasonable conditions on the acquisition of a communications device in light of established principles for the protection of privacy. Furthermore, the findings suggest that the issue is important in terms of public safety and security, but that the policy debate might be more fruitfully "reframed" (Schon & Rein, 1994) in terms of 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 as well as other communications devices (e.g., WiFi cards) on the grounds that they are neither reasonable nor appropriate measures for the purported benefit claimed.

Notes

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. The Australian regulations are not clear on the matter of telephone sharing or resale; however, the survey of Organisation for Economic Co-operation and Development (OECD) countries found that some, like Japan, in fact stipulate rules for transfer of ownership during resale of prepaid mobile phones (Gow, 2006).
3. 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 mobile phones and terrorism is suggestive of the way this link between anonymity and prepaid service 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, 2005).
4. Yet another way to identify a prepaid mobile phone is through its international mobile equipment identity (IMEI) number. This code is a 15-digit serial number that is uniquely stamped on a mobile phone device irrespective of the SIM card used.

References

Al Qaeda reivindica los atentados en un vídeo hallado en Madrid. (2004, March 14). *elmundo.es*. Retrieved April 14, 2004, from http://www.elmundo.es/elmundo/2004/03/13/espana/1079203-531.html

Australian Communications and Media Authority (ACMA). (2005). *Identity checks for pre-paid mobile services: Options for improvements to the collection and verification of identity information for prepaid mobile phone users*. Melbourne, Victoria, Australia: Author.

Australian Communications and Media Authority (ACMA). (2006). *ACMA considers improvements to identity check processes for pre-paid mobile phone customers*. Retrieved March 2006, from

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.

http://www.acma.gov.au/ACMAINTER.65654:STANDARD:1639069627:pc=PC_100468

Australian Communications Authority. (1997, December 22). *ACA makes rule applying to pre-paid mobile services* (Media Release No. 42 of 1997). Retrieved December 2003, from 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 February 2005, from http://internet.aca.gov.au/acainterwr/aca_home/legislation/radcomm/determinations/telecom/telspid_1of04.pdf

Bennett, C., & Regan, P. (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, from http://webuvic.ca/polisci/bennett/research/CPSA2002.htm

Bouc, F. (2005, February 24). Scratching out anonymity: Gov't proposes to ban anonymous prepaid mobile-phone SIMs. *The Prague Post*. Retrieved February 24, 2005, from http://www.praguepost.com/P03/2005/Art/0224/busi6.php

Dodds, P. (2005, July 29). Last suspects in failed bombings nabbed. *Guardian Unlimited*. Retrieved July 2005, from http://www.guardian.co.uk/worldlatest/story/0,1280,-5177074,00.html

European Digital Rights. (2004). *Polish proposal to demand ID for pre-paid cards*. Retrieved December 21, 2004, from http://www.edri.org/edrigram/number2.11/prepaid. Available from http://www.sfu.ca/cprost/prepaid/news/EDRI-Gram2-June2004Poland.htm

Furletti, M. (2004). *Prepaid card markets & regulation*. Philadelphia: Federal Reserve Bank of Philadelphia.

Government of Switzerland. (2003). *Conventions des Nations Unies pour la répression du financement du terrorisme et des attentats terroristes à l'explosif*. Retrieved July 10, 2007, from http://www.parlament.ch/afs/data/f/rb/f_rb_20020052.htm

Gow, G. A. (2005). Information privacy and mobile phones. *Convergence*, *11*(2), 75-87.

Gow, G. A. (2006). *Privacy rights and prepaid communication services: A survey of prepaid mobile phone regulation and registration policies among OECD member states*. (Research report for the Office of the Privacy Commissioner of Canada). Retrieved November 11, 2007, from http://www.sfu.ca/cprost/prepaid/

Kerr, I. (2007). *On the identity trail: Understanding the importance and impact of anonymity and authentication in a networked society*. Retrieved September 2007, from http://www.idtrail.org/

Lettice, J. (2003, March 12). Swiss move to block al-Qaeda mobile phone supply. *The Register*. Retrieved April 14, 2004, from http://www.theregister.co.uk/2003/03/12/swiss_move_to_block_al/

Lyon, D., & Stalder, F. (2003). Electronic identity cards and social classification. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and automated discrimination* (pp. 77-93). London: Routledge.

Majone, G. (1989). *Evidence, arguments, and persuasion in the policy process*. New Haven, CT: Yale University Press.

Marx, G. T. (1999). What's in a name? Some reflections on the sociology of anonymity. *The Information Society*, *15*, 99-112.

Marx, G. T. (2001). Identity and anonymity: Some conceptual distinctions and issues for research. In J. R. Caplan and J. Torpey (Eds.), *Documenting individual identity*. Princeton, NJ: Princeton University Press.

Microcell Telecommunications Inc. (2001). *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)*. Retrieved November 11, 2007, from http://www.crtc.gc.ca/PartVII/Eng/2001/8669/C12-01.htm

The mystery of Madrid's prime suspect. (2004, March 22). *The Australian*. Retrieved April 14, 2004, from http://www.theaustralian.news.com.au/common/story_page/0,5744,9036002%255E2703,00.html

Newman, A. (2004, March 16). Prepaid phones to reach 1.35 billion users by 2009. *infoSync World*. Retrieved April 13, 2004, from http://www.infosyncworld.com/system/print.php?id=4711

Office of the Privacy Commissioner of Canada. (2002). *Privacy Commissioner's reply comments regarding the "Lawful Access" proposals*. Retrieved April 19, 2004, from http://www.privcom.gc.ca/media/le_021125_e.asp

Organisation for Economic Co-operation and Development (OECD). (2005). *Communications outlook*. Paris: OECDpublishing.

Privacy Commissioner of Canada. (2000). *Personal information protection and electronic documents act*. Retrieved July 10, 2007, from http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

Privacy Commissioner of Canada. (2001). *PIPED Act Case Summary #24: Telephone company demands identification from new subscribers—Commissioner's findings*. Retrieved December 11, 2003, from http://www.privcom.gc.ca/cf-dc/cf-dc_011108_e.asp

Privacy International. (2004). Mistaken identity; exploring the relationship between national identity cards & the prevention of terrorism. Retrieved November 11, 2007, from http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf

Schon, D. A., & Rein, M. (1994). *Frame reflection: Toward the resolution of intractable policy controversies*. New York: Basic Books.

Swissinfo. (2004, March 4). *Swiss phone cards help trace al-Qaeda*. Retrieved April 14, 2004, from http://www.swissinfo.org/sen/Swissinfo.html?siteSect=111&sid=4763869

Thorne, J. (2005, August 1). High-tech tracked London Suspects. *The Christian Science Monitor*. Retrieved November 11, 2007 from http://www.csmonitor.com/2005/0801/p01s03-woeu.html

van Buuren, J. (2002). EU wants identification system for users of prepaid telephone cards. Retrieved December 20, 2004. Available from http://www.heise.de/tp/r4/artikel/12/12574/1.html

Wallace, K. (1999). Anonymity. *Ethics and Information Technology*, *1*, 23-35.

Weilenmann, A., & Larsson, C. (2001). Local use and sharing of mobile phones. In B. Brown, N. Green, & R. Harper (Eds.), *Wireless world: Social and interactional aspects of the mobile age*. London: Springer.

Gordon A. Gow is assistant professor in the graduate program in Communications and Technology at the University of Alberta. His research examines the social and policy implications of new communications technologies, with a specific emphasis on issues regarding wireless technology, public safety, and privacy rights.

Jennifer Parisi is a graduate student in the Department of Communication Studies at Concordia University. Her research interests include science, technology, and the right to privacy.

Downloaded from http://bst.sagepub.com at ALBERTA UNIVERSITY on May 7, 2008
© 2008 SAGE Publications. All rights reserved. Not for commercial use or unauthorized distribution.