



RESEARCH REPORT FOR
THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

Privacy Rights and Prepaid Communication Services

A survey of prepaid mobile phone regulation and registration
policies among OECD member states

CENTRE FOR POLICY RESEARCH ON SCIENCE AND TECHNOLOGY
SIMON FRASER UNIVERSITY VANCOUVER
March 2006



SIMON FRASER
UNIVERSITY
VANCOUVER



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

EXECUTIVE SUMMARY

This report sets out the results of responses to the Survey of Prepaid Mobile Phone Regulation and Registration Policies, issued for completion between April and October 2005. The survey outcome provides baseline data of the current state of regulation for prepaid mobile phones across international jurisdictions, principally those countries that are members of the Organisation for Economic Co-operation and Development (OECD).

The study was prompted in part by recent concerns about “anonymous” prepaid customers, following reports of terrorists using mobile phones to coordinate their activities and to detonate bombs. This is the first known effort to systematically gather information about the regulation of prepaid mobile phones across a range of countries.

The results of the survey are intended to contribute to an evidence-based policy deliberation on the issue of privacy rights and prepaid communications services in Canada and elsewhere.

The survey instrument itself was divided into several themes and contained questions related to each of the following areas:

- The regulation of prepaid mobile service or SIM cards in the country.
- Information about identity requirements for prepaid mobile phone service in the country.
- Background studies and codes of practice concerning the regulation and/or registration of prepaid mobile phones.
- Information about the presence and administration of an integrated public number database in the country.

Of the 24 countries that responded to the survey, nine have regulations that require mobile operators to collect customer information for

prepaid service: Australia, France, Germany, Hungary, Japan, Norway, Slovak Republic, South Africa and Switzerland.

In all cases, the rationale for a prepaid registration requirement was to improve efficiency of law enforcement and national security activities. In some countries the rationale is extended to include support for emergency services response and the commercial provision of public directory services. In a few cases, the requirement was raised in conjunction with specialized valued-added services (e.g., adult content, child minding); in certain cases, prepaid phone regulations are part of a wider legislative mandate that requires registration of all telephone services.

Australia is the only country known to have conducted a public consultation specifically about prepaid registration and it is expected that this consultation will produce empirical details that will continue to support a registration requirement. A public consultation on larger bodies of legislation that included prepaid phone registration has been held in Norway. Respondents indicated that there have been expert consultations in other countries, including Switzerland, Norway, and Japan but background studies or statistics pertaining to prepaid were not forthcoming.

Fifteen of the 24 countries that responded to the survey do not have an identity requirement; however, at least six countries considered and rejected a prepaid registration policy following a consultation process. These countries are Canada, Czech Republic, Greece, Ireland, the Netherlands and Poland. The UK respondent indicated that the UK government might have informally considered and rejected registration.

Various stakeholders in these countries have made comments that oppose prepaid registration. In Canada there have been

statements issued by the privacy commissioner's office, civil society groups, and mobile operators concerning problems with the requirements. A memo produced by the Mobile Broadband Group in the UK is the most detailed of these statements; opposition to the requirement includes cost, privacy rights, and effectiveness.

Where the registration of prepaid users is mandated, few reports have been published that oppose this legislation. However, there is evidence to suggest that a number of studies produced in Germany include findings that do not support prepaid registration, but these appear to be part of a wider critique of recent changes in legislation on data retention.

There is some documented evidence that assesses the capability and willingness of operators or regulators to monitor and enforce compliance in countries where a registration requirement has been introduced. For instance, in both Australia and Norway the issue of compliance has been a subject of ongoing discussion between the regulatory authority and industry stakeholders. In Switzerland there is an unconfirmed report which indicated that the service for unregistered prepaid customers was suspended after the deadline. In other countries, there is very little information that pertains to monitoring and compliance efforts either by government or mobile operators.

Regardless of whether or not registration has been legislated, there are few known cases of mobile operators voluntarily establishing prepaid registration as a corporate policy. In a number of cases, an incentive program is used to encourage prepaid customers to provide their personal details, but this is not intended for law enforcement or public safety purposes.

In countries where a registration policy is in effect, the general data collection requirements are specified in the regulations. Ireland is the only country where mobile operators developed an industry-wide code of practice, independent of government legislation. There was no information forthcoming from any country about

an industry code of practice to standardize the collection of customer data. One exception to this is in Australia, where the telecom industry in conjunction with the government has produced a technical document for collecting customer records for the integrated public number database.

There was no information forthcoming to suggest that alternative measures to identify prepaid users have been considered or used in most countries, with the exception of Germany and the Netherlands. Respondents from these countries indicated that IMSI (International Mobile Subscriber Identity)-catcher technology has been used. Australia has proposed an alternative to its "point of sale" identity verification with a "post-sale" electronic registration scheme. In Hungary, the prepaid phone's IMEI (International Mobile Equipment Identity) number, in addition to the SIM card number and the user's identity are recorded.

Australia is the only country known to have an active integrated public number database (IPND) system. In other countries, including Germany and the Netherlands, it was reported that mobile operators must maintain databases of customer records for law enforcement, but these are not integrated.

Australia has reported problems with prepaid phones and low quality customer records in the IPND; identity fraud and efficient verification remains a major challenge for the IPND in Australia. Privacy concerns have been raised in Australia about use and disclosure of customer data from the IPND despite the implementation of a detailed industry code of practice and standards to govern the use of the IPND system.

Although no empirical studies were located, the Australian regulator has issued opinions about the value of the IPND for law enforcement, public safety, as well as for child safety and for supporting competition in the provision of telecoms services (e.g., directory assistance, local number portability).

This report was prepared by Dr. Gordon Gow, Research Associate with the Centre for Policy Research on Science and Technology (CPROST) at Simon Fraser University. Dr. Gow is also a full-time Lecturer in the Department of Media and Communications at the London School of Economics and Political Science.

Jennifer Parisi from Simon Fraser University provided valuable research support throughout the course of the project and has assisted in preparation of this report as well with the ongoing maintenance of the project website:

<http://www.sfu.ca/cprost/prepaid/>

The author wishes thank all of those who participated in the study and who found time out of their busy schedules to respond to the questionnaire and follow up inquiries. Without their kind contributions this study would have been a much more difficult undertaking. The author also extends his appreciation to Richard Smith from CPROST and Lucie Menkveld from the School of Communication at Simon Fraser University for their tireless assistance in resolving administrative matters during the course of the study.

Finally, the author wishes to thank The Office of the Privacy Commissioner of Canada, under its 2005 Contributions Programme, for providing funding for this research.

LIST OF CONTRIBUTORS

John Mills
Investor Communications Manager
Telstra Corp Ltd
Australia

Austrian Regulatory Authority for Broadcasting
and Telecommunications
(Rundfunk und Telekom Regulierungs-GmbH)
Austria

Dielneus Dsabelle
Regulatory Affairs Manager
Belgacom Mobile NV
Belgium

Ken Huband
Director
Civil Liberties Association–National Capital Region
Canada

Henrik Udsen
Assistant Professor
University of Copenhagen
Denmark

Matthias Kießwetter
Legal Counsel, Bombardier
PhD Student, University of Münster
Germany

Kambouraki Dina, Kardasiadou Zoi
Auditors
Hellenic Data Protection Authority
Greece

Gabor Freidler
Office of the Parliamentary Commissioner for
Data Protection and Freedom of Information
Hungary

Ernesto Villanueva Villanueva
President
LIMAC (Libertad de Informacion
Mexico, AC)
Mexico

Blair Stewart
Assistant Commissioner
Office of the Privacy Commissioner
New Zealand

Thomas Olsen
Research Fellow
Section for IT and Administrative Systems
University of Oslo
Norway

Dorota Skolimowska
Legal Department Director
Bureau of the Inspector General for Personal
Data Protection
Poland

Christina Minoia Perez
Head of Legal
Vodafone Portugal
Portugal

Daniel Valentovic
International Relations Manager
The Office for Personal Data Protection of the
Slovak Republic
Slovak Republic

Mathias Klang
Lecturer
University of Göteborg
Sweden

Jim Dempsey
Executive Director
Center for Democracy and Technology
USA

CONTENTS

EXECUTIVE SUMMARY	1	Norway (NO)	41
		Poland (PL)	44
FOREWORD	3	Portugal (PT)	45
		Slovak Republic (SK)	45
LIST OF CONTRIBUTORS	4	South Africa (non-OECD)	47
List of Tables	6	Spain (ES)	48
List of Figures	6	Sweden (SE)	50
		Switzerland (CH)	50
PART I	7	Turkey (TR)	52
Purpose and Objectives	7	United Kingdom (UK)	53
Prepaid Mobile Phone Service in Canada	8	United States (US)	55
Prepaid Mobile Phone Service around the World	10	SUMMARY	57
Privacy Rights and Prepaid Mobile Phones A Test of Reasonable Appropriateness	12 16	Justification for and against prepaid registration	57
		Feasibility of implementing and enforcing regulatory measures	57
		Possible use of alternative measures	58
		Impact on IPND	58
PART II	19	ANNEX A: SURVEY INSTRUMENT	59
Survey Design	19	ANNEX B: SUMMARY OF RESPONSES TO THE SURVEY	61
General Observations	20	ANNEX C: VODAFONE JAPAN CUSTOMER NOTIFICATION	69
Individual Country Profiles	23	About Vodafone K.K.	69
Australia (AU)	23	ANNEX D: TRANSLATION OF NPT LETTER OF 29 SEPTEMBER 2004	70
Austria (AT)	27	ANNEX E: TRANSLATION OF NPT LETTER OF 8 NOVEMBER 2004	73
Belgium (BE)	27	ANNEX F: SWISSCOM CUSTOMER NOTIFICATION	75
Canada (CA)	28	ANNEX G: SWISSCOM CUSTOMER REGISTRATION FORM	76
Czech Republic (CZ)	29		
Denmark (DK)	30		
Finland (FI)	30		
France (FR)	30		
Germany (DE)	31		
Greece (GR)	34		
Hungary (HU)	35		
Iceland (IS)	36		
Ireland (IE)	36		
Italy (IT)	37		
Japan (JP)	37		
Korea (KR)	39		
Luxembourg (LE)	39		
Mexico (MX)	39		
Netherlands (NL)	40		
New Zealand (NZ)	41		

Table 1: Growth of Prepaid Mobile Phones in Canada 2000-2005	8	Figure 1: Sasktel Mobility Prepaid Card	9
Table 2: Major Canadian Mobile Operators and Prepaid Subscriptions	8	Figure 2: Political cartoon about the Swiss ban “anonymous” prepaid phones.	15
Table 3: Prepaid Mobile Phones in the OECD	10	Figure 3: Notice to Vodafone Japan customers	17
Table 4: Growth of Prepaid Subscribers Globally 2004-2010	11		

Purpose and Objectives

The growth of mobile telephone service in Canada and around the world has been phenomenal, with much of that growth directly attributable to the adoption of prepaid (“pay-as-you-go”) plans. Prepaid phones today represent a significant and growing percentage of the domestic and international mobile phone markets.

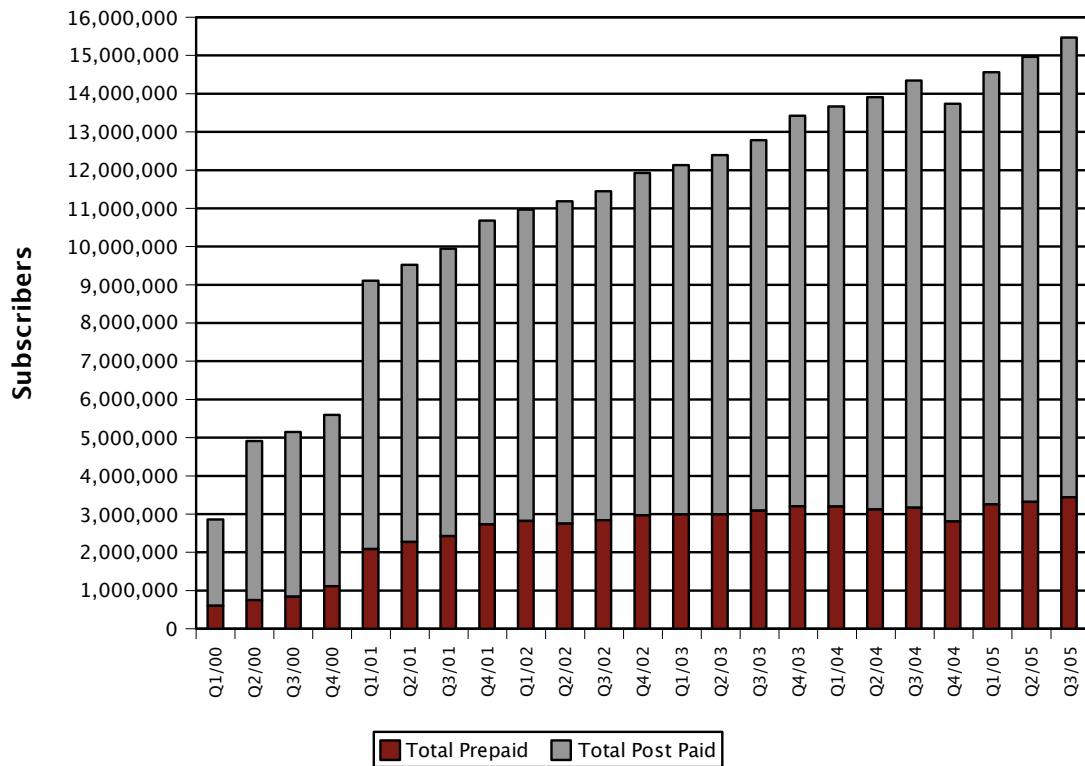
While this development has been hailed as a marketing success in the provision of competitive telephone service, it also has raised concerns within the law enforcement community about the possible use of “anonymous” prepaid mobile phones for criminal or terrorist activities. In response, a number of countries have passed laws to require mobile carriers to collect personal information from their prepaid mobile phone customers as a condition of service. Canada has not yet introduced such regulations and it is not clear that it will do so in the future.

Nevertheless, the possibility of prepaid registration ought to be a matter of interest for the Office of the Privacy Commissioner because the legal and ethical implications of such a measure remain uncertain. Moreover, public deliberation on both sides of the issue in Canada has been encumbered by a lack of information about what objectives such a requirement might realistically seek to achieve or how it might be implemented and enforced.

The purpose of this survey is to address this information gap by gathering details on the current state of regulation of prepaid mobile phones across a comparable range of countries in the OECD.

This report presents the results of the survey and is intended to contribute to an informed public deliberation on the question of privacy rights and prepaid communications services in Canada and elsewhere.

Cellular/PCS Subscriber Type in Canada



Source: Canadian Wireless Telecommunications Association

Table 1: Growth of Prepaid Mobile Phones in Canada 2000-2005

	2003	2004	2005 (Q2)
Aliant Mobility	--	--	78,145 (11.7%)
Bell Wireless Alliance	1,178,705 (23.6%)	1,320,761 (23.8%)	1,193,855 (26.9%) ¹
Microcell (Fido)	652,966 (52.4%)	545,911 (42.8%) ²	--
Rogers Wireless	759,990 (20.0%)	792,300 (14.3%)	1,317,900 (23.1%)
TELUS Mobility	611,680 (17.8%)	696,100 (17.6%)	728,700 (17.5%)
TOTAL	3,203,341 (23.8%)	2,809,161 (18.7%)	3,318,600 (21.2%)

Source: Canadian Wireless Telecommunications Association

Table 2: Major Canadian Mobile Operators and Prepaid Subscriptions

Prepaid Mobile Phone Service in Canada

Prepaid mobile phone service in Canada represents an important segment of the consumer market. Figures collected by the Canadian Wireless Telecommunications Association (CWTA) show that demand for prepaid service has remained consistent since 2002.

¹ Includes Bell Mobility, NorthernTel Mobility, Télébec Mobility and the proportionate share of the Virgin Mobile Canada joint venture.

² Microcell data provided up to Q2 only. Rogers Wireless acquired the company in 2004.

As shown in Table 1, prepaid mobile phones account for just over 20 per cent of the total mobile phone market in Canada, which translates to about 3.3-million individual subscriptions. Table 2 provides details of the major wireless service providers in Canada, showing total number of prepaid subscribers for each, as well as the percentage of prepaid in relation to the total subscriber base for each carrier.

According to the most recent publicly available figures, Bell Wireless Alliance holds the greatest percentage of prepaid accounts measured against its total subscription base, at 26.9 per cent. Rogers Wireless, however, has a larger total number of prepaid customers at 1.3-million, though this amounted to a smaller percentage of its total subscription base.

Consumer demand for prepaid service is due partly to the ease with which it can be purchased in combination with its widespread availability in retail outlets, grocery stores, gas stations, and so forth. Customers with credit problems or those otherwise concerned about managing monthly costs might consider prepaid an affordable means of obtaining telephone service. Business owners might choose prepaid phones for their employees as a cost management strategy or to avoid committing to long-term contracts with service providers. Parents might wish to purchase prepaid mobile phones for their children as a means of staying in touch and controlling cost. Others might purchase a prepaid phone with the intent of using it only for emergencies. A 2002 industry report on prepaid wireless in the United States identified a number of target customer segments:³

- Low-credit customers
- Occasional users wanting to avoid contracts
- Teenagers and young adults
- Certain ethnic groups and immigrants
- Transient travellers

3 Katz, Raul, Riddleberger, Eric, Sarma, Bharat, et al. (2002). Prepaid Wireless: the Next Frontier in the U.S. Wireless Industry. Booz, Allen, Hamilton Publications.

When acquiring prepaid service customers usually purchase a mobile handset bundled with airtime credit. Purchase of both the handset and additional airtime credit can be done with cash, cheque, debit or credit card transaction. Handsets and airtime credit vouchers are sold through a wide range of distribution channels, with airtime credit purchased in blocks of minutes or in cash value denominations. In some countries, airtime credit can be purchased through automated teller machines or by electronic transaction over the Internet.



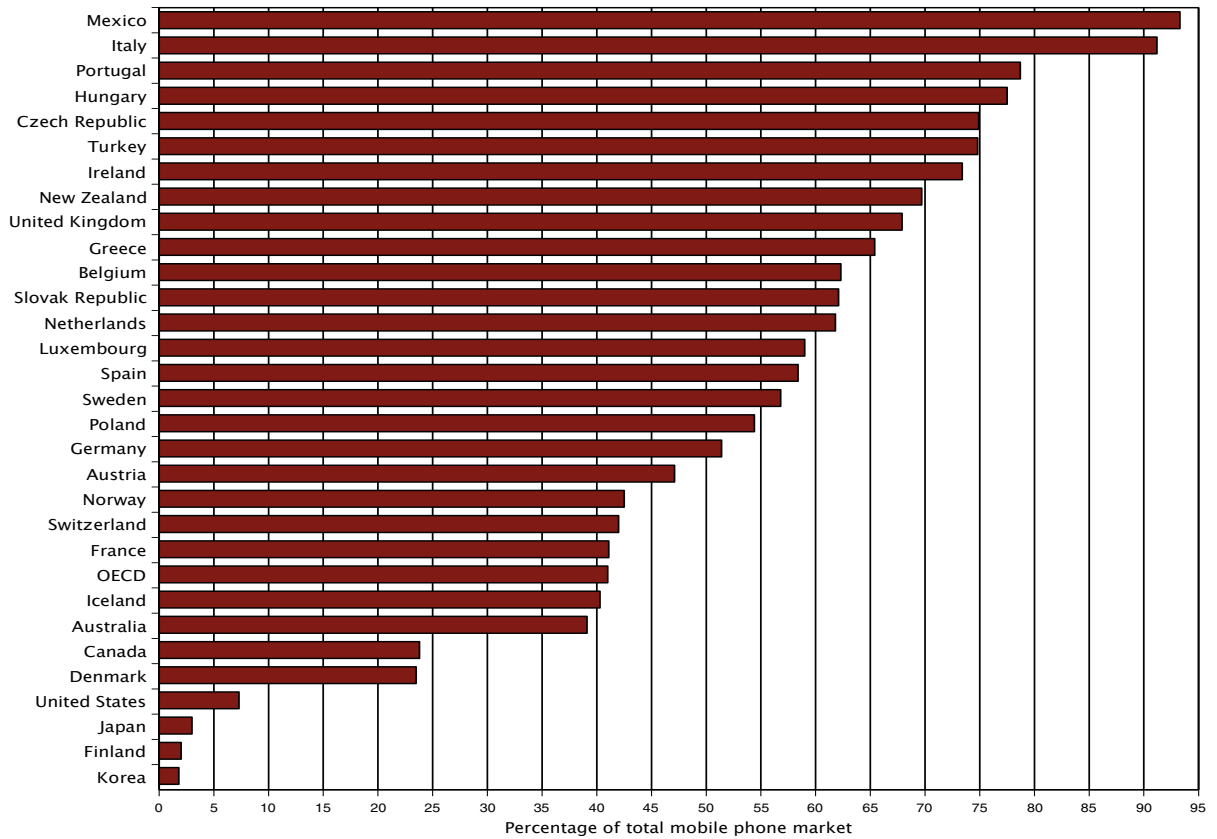
Source: Sasktel Mobility website. http://www.sasktelmobility.com/productsservices/cellular/images/prepaid_100_card.jpg

Figure 1: Sasktel Mobility Prepaid Card

When a prepaid phone is used to make calls, the service provider debits the airtime credit according to time used and the type of call that is made (e.g., long distance or local). In most cases, prepaid accounts also have an expiry date associated with the activation of each airtime credit voucher. The expiry date can vary from 30 days to several months depending on the service provider.

In Canada and in other countries mobile operators have agreed to accept 9-1-1 dialled emergency calls from all mobile phones irrespective of the subscriber's account standing. This agreement includes prepaid accounts or otherwise inactive prepaid mobile phones (provided of course that the phone is in working order).

Prepaid mobile phones in the OECD (2003)



Source: OECD Communications Outlook 2005

Table 3: Prepaid Mobile Phones in the OECD

Prepaid Mobile Phone Service around the World

Prepaid represents a significant share of the global mobile phone market, although this varies widely from country to country. Table 3 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 countries is Mexico, where over 90 of the mobile phone market is prepaid. South Korea is at the bottom of the ranking with almost no reported prepaid service in that country. In the EU, Italy tops the ranking at over 90 per cent and Portugal follows with prepaid customers making up almost 80 per cent of the total mobile phone market. Finland is the lowest ranked EU country with less than five per cent of customers choosing prepaid. In the United States, prepaid is less than ten per cent of the market, whereas Canada is similar to

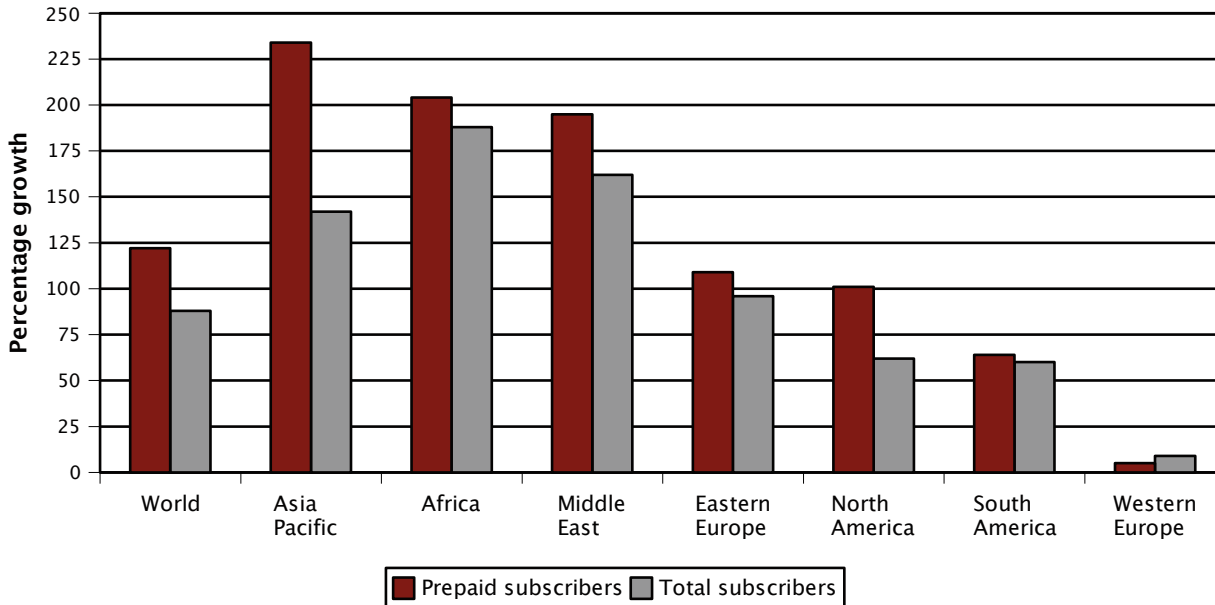
Denmark, with prepaid holding just over 20 per cent of total market share.

Looking ahead, industry forecasts suggest that the prepaid market will grow to reach some 1.35-billion subscribers by 2009. This translates to about 59 per cent of the total global wireless market.⁴ 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.

4 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>

Growth of prepaid customers compared with total growth 2004-2010



Source: Baskerville Global Mobile Prepaid Strategies and Forecasts (2003)

Table 4: Growth of Prepaid Subscribers Globally 2004-2010

- Most markets continue to actively promote prepaid service, 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.⁵

Prepaid mobile phones are one category within a larger market of “stored value cards” that also

include gift cards, travel cards, and payroll cards. A 2004 report issued by the Federal Reserve Bank of Philadelphia suggests that the overall market for stored valued 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.).⁶

5 Baskerville (2003). Global Mobile Prepaid Strategies and Forecasts. Informa Telecoms Group.

6 Furletti, Mark. (2004). Prepaid Card Markets & Regulation. Philadelphia: Federal Reserve Bank of Philadelphia. (p. 9)

Attempts to regulate a growing “stored value” card market could lead to proposals for merchants to collect and register customer information for other types of prepaid services besides prepaid mobile phones, to prevent fraud or to address other legal concerns.

Privacy Rights and Prepaid Mobile Phones

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 9-1-1.⁷ 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 described elsewhere as the “first domain” of location privacy research.⁸

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 rights issue centres on 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 when activating the service. This issue has not been extensively examined in the literature on information privacy, perhaps in part because prepaid mobile phone service is a new business model. Nevertheless, it raises an interesting question for privacy studies: should there be an entitlement to anonymity in the ownership and use of a telephone? This question extends to a wider issue that goes beyond “plain old telephone service” and considers 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, is there a legitimate claim 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 study is not to delve into the bigger issue per se but rather to provide empirical evidence with which to examine the issue as it relates to mobile phones, and with the secondary intent of contributing to a wider public policy debate on the matter.

A debate over prepaid mobile phones and the anonymity question surfaced initially in Canada during the Wireless E911 proceedings. The substance of these proceedings was the design and deployment of an “enhanced” emergency service for mobile phones. Similar to the initiative 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.

During the Canadian proceedings, one mobile operator revealed that a significant proportion of its customer base was prepaid and that it would not be feasible to provide the kind of detailed customer information that some public safety organizations were seeking for the E911 service. The mobile operator stated in its remarks to the Canadian regulator that prepaid

7 Regan, Priscilla, Bennett, Colin and Phillips, David. (2002, Sept. 28-30). Emergent Locations: Implementing Wireless E9-1-1 in Texas, Virginia, and Ontario. Paper presented at the Telecommunications Policy Research Conference, Alexandria, Virginia.

8 Gow, Gordon A. (2005). Information Privacy and Mobile Phones. *Convergence*, 11(2), 75-87.

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 it 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.⁹

From the perspective of this mobile operator, the collection of customer information in the form of a home or business address is considered irrelevant to locating a mobile 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.¹⁰

Prior to making this statement, the public safety agencies had 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.¹¹

Further inquiry into this matter has revealed that concern about "anonymous" prepaid customers has surfaced in other countries, especially following reports of terrorists using mobile phones to coordinate their activities and to detonate bombs. In 2004, for instance, the *New York Times* reported that law enforcement authorities had intercepted an al-Qaeda terrorist cell using prepaid mobile phones issued by a Swiss mobile operator.¹² The Madrid bombings in

9 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>

10 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>

11 Microcell Telecommunications Inc. (2002, Jan. 17). 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 I - 2001/01/17 - Microcell Telecommunications Inc. Available <http://www.crtc.gc.ca/PartVII/Eng/2001/8669/C12-01.htm>

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

2004 were also linked to prepaid mobile phones that were allegedly used as detonators.¹³

Earlier, 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 in this case 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.”¹⁴ 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. The following sample of comments illustrate this growing concern prepaid mobile 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, 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 law enforcement has confidence in a database for emergency calls.” —Executive from Australia telecom industry

There is opposition to such regulatory measures, however, particularly by those who question the feasibility of a prepaid registration requirement. This is a position characterized, or rather satirized, by John Lettice, writing for the UK-based mobile communications news source *The Register*:

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 referring to the Swiss requirement to register prepaid SIM cards (i.e., mobile phones) for law enforcement purposes:

13 Al Qaeda reivindica los atentados en un vídeo hallado en Madrid. (2004, March 14). [elmundo.es](http://www.elmundo.es/elmundo/2004/03/13/espana/1079203531.html). Retrieved Apr. 14, 2004. Available <http://www.elmundo.es/elmundo/2004/03/13/espana/1079203531.html>; 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>.

14 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>

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...¹⁵

Lettice, like a number of privacy rights advocates and mobile operators, believes that a registration requirement is futile 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.

Figure 2 shows a political cartoon published in *Nebelspalter* magazine in response to the Swiss government decision to ban "anonymous" prepaid mobile phones in 2004. The cartoonist is suggesting that a registration requirement will lead criminals to resort to identity fraud to obtain prepaid phones. In the drawing, a hand reaches out from a dark alley way, tempting a young passerby with cash: "Psst ... Kid! I'll give you some money if you buy me a prepaid card using your name."



Source: Cartoon by Silvan Wegmann, published in *Nebelspalter* magazine; http://www.nebelspalter.ch/magazin/archiv/archiv_2003/04/prepaid.htm

Figure 2: Political cartoon about the Swiss ban "anonymous" prepaid phones.

¹⁵ 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/

A Test of Reasonable Appropriateness

One way to frame the question of prepaid phones and privacy rights 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 collection of 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.¹⁶

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.¹⁷ 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.

It does not appear to be the case that the Privacy Commissioner has 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.¹⁸

If considered against section 5.3 of the PIPED Act, this “gross invasion of privacy” would stem in part from the view 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 claims associated with a call for prepaid registration in Canada’s Lawful Access Consultations in 2002 (Office of the Privacy Commissioner of Canada, 2002). Moreover, an initial investigation conducted for this report was unable to identify published studies that either

16 Privacy Commissioner of Canada. (2000). Personal Information Protection and Electronic Documents Act. Available http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

17 Privacy Commissioner of Canada. (2001, Nov. 8). PIPED Act Case Summary #24: Telephone company demands identification from new subscribers. Commissioner’s Findings. Available http://www.privcom.gc.ca/cf-dc/cf-dc_011108_e.asp

18 Office of the Privacy Commissioner of Canada. (2002, Nov. 25). Privacy Commissioner’s reply comments regarding the “Lawful Access” proposals. Available http://www.privcom.gc.ca/media/le_021125_e.asp

establish a clear link between prepaid mobile phones and telephone-based criminal/terrorist activity, or that establish a link between the introduction of a prepaid registration policy and a corresponding reduction in telephone-based criminal/terrorist activity.

On the other hand, it might not be necessary to produce such evidence and still present a politically and socially acceptable case for adopting a registration policy for prepaid phones. Such a case could be based on an interpretation of existing legislative authority and/or an efficiency argument that claims such regulation will improve the efficiency of law enforcement and public safety undertakings.¹⁹



Source: Vodafone Japan. <http://www.vodafone.jp/english/products/index.html>

Figure 3: Notice to Vodafone Japan customers

Critics, however, might present an equally compelling argument to suggest that claims about the efficiency gains of registration are fallacious, and that alternative methods of identifying telephone users are more effective. For example, this is the position taken in a memo drafted by the UK-based Mobile Broadband Group where it is argued that a registration policy is an expensive strategy of little practical effect. This position therefore tends to support

the claim to “anonymous” ownership and use of prepaid mobile phones both on the authority of existing privacy legislation and also on an efficiency argument (i.e., prepaid registration is *not* an efficient strategy).

One aim of this study is to support an informed public deliberation about this notion of “reasonable appropriateness” as it pertains to a prepaid registration policy in Canada and elsewhere. More specifically, the primary motivation for the survey has been to generate empirical evidence on the regulation of prepaid mobile phones in countries similar to Canada.

The importance of having such evidence on hand during deliberations is reinforced by the potential problem of making improper inferences drawn from anecdotal reports in the media and elsewhere. For instance, in a widely read book on the policy process, Giandomenico Majone has noted the persistent and often unexamined problem of logical fallacies, or pitfalls that sometime pervade 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.²⁰

19 Baldwin, Robert and Cave, Martin. (1999). *Understanding Regulation: Theory, Strategy, and Practice*. New York: Oxford University Press. (p. 77-81).

20 Majone, Giandomenico. (1989). *Evidence, Arguments, and Persuasion in the Policy Process*. New Haven: Yale University Press (p. 52).

Majone specifies that a pitfall is not a simple error in procedure or in factual evidence, but instead stems from a more fundamental flaw in the basic structure of an argument supporting a proposed solution or approach. The intent of the study has not been to carry out an in-depth analysis of the findings, but rather to present a baseline of information to help policymakers and others avoid some of the pitfalls that might otherwise encumber public debate on the question of prepaid communications and privacy rights in Canada and elsewhere.

Survey Design

The survey was designed to gather information related to five primary research questions:

1. What is the **justification** and related evidence to support regulatory measures **to eliminate** the sale of ‘anonymous’ prepaid mobile phone service in countries similar to Canada?
2. What is the **justification** and related evidence to support regulatory measures **to protect** the sale of ‘anonymous’ prepaid mobile phone service in countries similar to Canada?
3. What is the **feasibility** of implementing and enforcing regulatory measures intended to eliminate the sale of anonymous prepaid mobile phone service in countries similar to Canada?
4. If regulatory measures are not feasible then what type of **alternative measures** have been or might be adopted to achieve similar ends?
5. If anonymous prepaid mobile phones continue to be permitted then what impact might this have on the accuracy and usefulness of any form of **integrated public number database**, either planned or envisaged, in countries similar to Canada?

The survey instrument itself was divided into five themes and contained questions related to each of the following areas:

- **Part A:** The regulation of prepaid mobile service or SIM cards in your country.
- **Part B:** Information about identity requirements for prepaid mobile phone service in your country.
- **Part C:** Background studies and codes of practice concerning the regulation and/or registration of prepaid mobile phones.
- **Part D:** Information about the presence and administration of an integrated public number database in your country.
- **Part E:** Additional comments and contact information.

Responses to the survey have come from a diverse range of participants including mobile phone operators, academic experts, and government officials. In some cases, additional information was drawn from material gathered by the research team. This material included media reports as well as industry and government documents.

General Observations

The following matrices provide a comparison of observations plotted against a series of indicators. These indicators formed part of the interpretive structure that was used to analyze responses to the survey questions in relation to the research questions. The intent here is to present general observations derived from the 26 countries that responded to the survey.

<i>What is the justification and related evidence to support regulatory measures to eliminate the sale of ‘anonymous’ prepaid mobile phone service in countries similar to Canada?</i>	
Indicators	Observations
Number of countries that have introduced identity requirements for prepaid mobile phone service (A1)	9 countries out of 24 that have responded to the survey have introduced an identity requirement for prepaid; one country that did not participate in the survey has allegedly introduced a prepaid registration policy (Italy) although this is not confirmed.
Public statements concerning the need for such requirements (A2)	In all cases, the rationale for a prepaid registration requirement was to improve efficiency of law enforcement and national security activities; in some countries the rationale is extended to include support for emergency services response and the commercial provision of public directory services; in a few cases, the requirement was raised in conjunction with specialized valued-added services (e.g., adult content, child minding); in certain cases, prepaid phone regulations are part a wider legislative mandate that requires registration of all telephone services.
Existence of background studies or statistics that support such requirements (A3, B1)	Australia is the only country known to have conducted public consultations specifically about prepaid registration; it is expected that this consultation will produce empirical details that will continue to support a registration requirement; a public consultation on larger bodies of legislation that included prepaid phone registration has been held in Norway; respondents indicated that there have been expert consultations in other countries, including Switzerland, Norway, and Japan but background studies or statistics pertaining to prepaid were not forthcoming.

What is the **justification** and related evidence to support regulatory measures **to protect** the sale of ‘anonymous’ prepaid mobile phone service in countries similar to Canada?

Indicators	Observations
Number of countries that continue to permit the sale and use of anonymous prepaid mobile phones service (A1)	15 of the 24 countries that responded to the survey do not have an identity requirement; however, at least 6 countries considered and rejected a prepaid registration policy following a consultation process; these countries are Canada, Czech Republic, Greece, Ireland, the Netherlands and Poland; the UK respondent indicated that the UK government might have informally considered and rejected registration.
Public statements concerning the problem with such requirements (A2)	In Canada there have been statements issued by the Privacy Commissioner’s office, civil society groups, and mobile operators concerning problems with the requirements; of the countries responding to the survey, a memo produced by the Mobile Broadband Group in the UK is the most detailed statement opposing registration requirements; opposition to the requirement includes cost, privacy rights, and effectiveness.
Existence of background studies or statistics that do not support such requirements (A3, C1)	There is evidence to suggest that a number of studies produced in Germany include findings that do not support prepaid registration, but these appear to be part of a wider critique of recent changes in legislation on data retention.

What is the **feasibility** of implementing and enforcing regulatory measures intended to eliminate the sale of anonymous prepaid mobile phone service in countries similar to Canada?

Indicators	Observations
Evidence of capability and willingness of designated organizations to monitor and enforce compliance (B2, B3, B4, B5)	There is some documented evidence to assess the capability and willingness of operators or regulators to monitor and enforce compliance in countries where a registration requirement has been introduced; for instance, in both Australia and Norway the issue of compliance has been a subject of ongoing discussion between the regulatory authority and industry stakeholders; in Switzerland there is an unconfirmed report indicated that the service for unregistered prepaid customers was suspended after the deadline; in other countries there is little available information pertaining to monitoring and compliance efforts either by government or mobile operators.
Existence of voluntary corporate policy for collecting customer information (C2)	There are few known cases where a mobile operator requires prepaid registration as a corporate policy (in contrast to it being a regulatory requirement); In a number of cases, an incentive program is used to encourage prepaid customers to provide their personal details, but this is not intended for law enforcement or public safety purposes.
Existence of industry voluntary code of practice related to collection of customer information (C3)	In countries where a registration policy is in effect, the general data collection requirements are specified in the regulations; Ireland is the only country where mobile operators developed an industry-wide code of practice, independent of government legislation; there was no information forthcoming from any country about an industry code of practice to standardize the collection of customer data; one exception to this is in Australia, where the telecom industry in conjunction with the government has produced a technical document for collecting customer records for the integrated public number database.

*If regulatory measures are not feasible then what type of **alternative measures** have been or might be adopted to achieve similar ends?*

Indicators	Observations
Potential use of alternative methods to identify prepaid mobile customers (A4)	There was no information forthcoming to suggest that alternative measures to identify prepaid users have been considered or used in most countries, with the exception of Germany and the Netherlands; respondents from these countries indicated that IMSI-catcher technology has been used; the UK respondent mentioned specialized databases for tracking stolen mobile phone equipment; Australia has proposed an alternative to its “point of sale” identity verification with a “post-sale” electronic registration scheme; In Hungary, the prepaid phone’s IMEI number, in addition to the SIM card number and user’s identity are recorded.
Documented use of technical methods to identify prepaid mobile phone customers (A5)	German respondent provided source details for documented evidence of IMSI-catcher technology being used in that country to identify mobile phone customers.


*If anonymous prepaid mobile phones continue to be permitted then what impact might this have on the accuracy and usefulness of any form of **integrated public number database**, either planned or envisaged, in countries similar to Canada?*

Indicators	Observations
Size of the prepaid market in the country	There is no correspondence with the extent of the prepaid market in a country and the existence of an IPND system.
Existence of IPND in a country (D1)	Australia is the only country known to have an active IPND system; in other countries, including Germany and the Netherlands, it was reported that mobile operators must maintain databases of customer records for law enforcement, but these are not integrated.
Reported experience with an IPND in a country (D2)	Australia has reported problems with prepaid phones and low quality customer records in the IPND; identity fraud and efficient verification remains a major challenge for the IPND in Australia; privacy concerns have been raised in Australia about use and disclosure of customer data from the IPND; Australia has developed an industry code of practice and standards to govern the use of the IPND system.
Statements about prospective usefulness of an IPND in a country (D3, D4)	No empirical studies were located, but the Australian regulator has issued opinions about the value of the IPND for law enforcement, public safety, as well as for child safety and for supporting competition in the provision of telecoms services (e.g., directory assistance, local number portability).

Individual Country Profiles

The following section provides detailed information on each country that was asked to respond to the survey. The table accompanying each profile includes the most recent OECD statistics on prepaid mobile phone service in that country, showing the number of subscribers and percentage share of the total mobile phone market. The arrows indicate the net change in the prepaid market from 2002 to 2003.

Australia (AU)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
3,339 (30%)	3,339 (26.6%) ↓	5,606 (39.1%) ↑

Source: OECD (2005) *Communication Outlook*.

The government of Australia requires telecom service providers to collect and retain customer information for all types of subscriptions including prepaid mobile phone service. This requirement was first introduced in 1997 and subsequently amended in 2000 to become *Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*. Two further amendments to the Determination were adopted in 2004 to provide mobile operators with flexible identity collection procedures.

The prepaid registration requirement is enacted as a “Determination” by the Australian Communications and Media Authority (ACMA), which stems from a provision in the Australian Telecommunications Act Section 99(1) that permits the regulator to establish specific obligations of mobile operators, referred to as “Carriage Service Providers” (CSPs) in the legislation.

Other sections of the Telecommunications Act relevant to the prepaid policy include Part 14, which requires mobile operators to provide assistance to law enforcement and national security agencies. As such, “a vital part of each

[carrier’s] preparations to assist law enforcement agencies is to maintain accurate records of their customer’s personal details.” Part 4 of Schedule 2 of the Act stipulates that all mobile operators contribute to the maintenance of a national Integrated Public Number Database, which means collecting and validating basic personal information for all customers, including prepaid subscribers. Further to this obligation, the ACMA *Telecommunications (Emergency Call Service) Determination 2000* requires mobile operators to ensure the validity of all customer records provided to the IPND administrator to support emergency call service.²¹

In February 2005, the ACMA initiated a review of its prepaid policy, leading to a discussion paper in July and culminating in a public consultation planned for September 2005. The review has been launched to address a number of shortcomings with the current registration requirement; namely, a concern with improving the accuracy of end-user information that is collected by mobile operators, balanced against the constraints imposed by a wide (and growing) range of distribution channels for prepaid mobile phones.

In the July discussion paper, the ACMA explains the policy objective of the prepaid regulations:

... the key objective of the Determination is to ensure the collection and maintenance of accurate identity data for consumers of prepaid mobile services in order to provide accurate information about consumers of prepaid services in order to assist law enforcement and national security agencies in their investigations, emergency service organisations in their responses to emergency situations and public number

21 Australian Communications and Media Authority. (2005, July). *Identity Checks for Pre-paid Mobile Services: Options for improvements to the collection and verification of identity information for prepaid mobile phone users*. Melbourne. (p. 10)

directory producers in their production of useful directories.²²

The central purpose of the review has been to seek consensus on a further amendment to the Determination. This amendment would provide for an alternative identification process that does not depend on the collection of personal information at the point of sale, also known as the “Part 3” method. The original Determination requires that mobile operators collect and verify prepaid customer information at the point-of-sale for all purchases made other than by credit or debit card. Verification is performed with a document such as a passport or birth certificate that is to be examined and confirmed by a retail sales agent.²³

In 2004 the original Determination was replaced with an amendment that retained the “Part 3” method but also included an alternative “Part 4” method for the identity check. This alternative method allows mobile operators to verify customer identification using a database maintained by the mobile operator or another party. In effect, it provides for an online or telephone-based verification procedure that does not necessitate a physical examination of the identifying documents at the point-of-sale and can therefore be done “post-sale.” However, as the ACMA has noted, the Part 4 method has yet to be widely adopted by the mobile industry in Australia:

Implementation of the Part 4 process was focussed on obtaining access to a robust, single data source against which

carriers and CSPs could verify customer data post-sale. Access to a single data source was not forthcoming. As a result, CSPs continued to use the Part 3, point of sale, identity verification process.²⁴

In May 2004, the ACMA once again amended the Determination to allow mobile operators to seek approval of any alternative compliance plan to qualify as a “Part 4A” method. No such plans have so far been approved by the ACMA. In sum, the Determination provides three alternative procedures for identifying prepaid customers but industry continues to operate using the original Part 3 method.

The current review of the Determination has been prompted by the ACMA’s recognition of a number of concerns. These concerns are noted in the July 2005 discussion paper.²⁵

- *Compliance in distribution networks:* ACMA jurisdiction extends to mobile operators but not to the retail dealers and agents that often sell prepaid services to consumers. The ACMA notes that existing contractual arrangements between mobile operators and their dealers “are not always effective in securing compliance with the requirements under the Determination.”
- *Quality of data collected:* the current Determination Part 3 method often leads to a duplication of information collection, once at the point of sale and again during the service activation procedure as required by law for the maintenance of the Integrated Public Number Database (IPND). Whereas verification is required at the point of sale it is not required during the activation process, leading to a problem of unverified data being included in the IPND. The ACMA has noted several concerns arising from this situation; namely, that the two step procedure is an inefficient business practice and that “it invites evasion by those seeking to remain anonymous for criminal purposes.”

22 *ibid.* (p. 12)

23 The ACMA discussion paper makes an important distinction between *validation* and *verification* of documents. Identity validation refers to a procedure to check that the information provided may be true. For example, to validate a customer’s claim that they reside at “345 Hornby Street, Vancouver” means to check if there is a “Hornby Street” in Vancouver and to check if there is a building with the number “345.” Validation of customer details is routine procedure for entry into the E911 databases in Canadian cities. Verification, on the other hand, is a procedure to check that the information provided *is* true; in other words, that the customer is in fact who they profess to be and that they do in fact reside at the address given.

24 *ibid.* (p. 13)

25 *ibid.* (p. 13-15)

- *IPND accuracy*: recent audits of the IPND in Australia have revealed low accuracy of mobile service records compared with fixed line service. In addition, reports to the ACMA indicate that the quality of prepaid customer records in the IPND is “significantly poorer” than that for post-paid mobile phone customer records. This has led the ACMA to conclude that adequate identity checks are not being performed during prepaid mobile service activation.
- *Industry costs*: the ACMA recognizes that significant costs are incurred to ensure compliance with the Part 3 method. Costs include the provision of training and administration of the identity checking process at the retail level; the hiring of agents to monitor compliance among retailers; enforcing compliance; and archiving identity documents. The point of sale method also leads to missed revenue opportunities because it inhibits the mobile industry from attempting to distribute prepaid by innovative means, such as through vending machines.
- *Consumer privacy*: the current Part 3 method raises privacy concerns because it often means that customers must provide personal details and documents in a retail environment “in which they may not have confidence that their privacy and identity information will be safeguarded.” Furthermore, the IPND obligation means that customers often must submit their details again during the service activation procedure.
- *Public safety*: the current Part 3 method does not require mobile operators to verify customer information during the service activation process. It is the information collected during the activation process that is provided to the IPND, which is used for both law enforcement and emergency services dispatch. Inaccuracies in the IPND can in turn create delays in emergency services operations during life-threatening or time critical situations.

To address these concerns, the ACMA has proposed in its discussion paper a long-term solution that would eliminate the point of sale

identity check altogether. Instead, the Part 4 method would remain but in an expanded form, with the ACMA to consider a range of options for electronic “point of activation” identity checks for mobile operators. The renewed interest in the Part 4 method seems to have been prompted by “advances in data matching systems” to combat identity fraud, including Australian government initiative to develop a national “online document verification system” (DVS).

The ACMA proposes a method by which mobile operators would have access to either a government or industry data matching system for real-time verification of customer identity documents. While the ACMA estimates that its proposal is subject to many practical constraints and would be at least two years away from realization in any form, it also suggests that it might be an acceptable strategy for dealing with concerns stemming from the current Part 3 method:

Preliminary consultation undertaken to date with key stakeholders indicates strong multi-lateral support for utilising the [Document Verification System] to provide for a real-time, online identity verification process undertaken at point of activation of a prepaid service, as long as adequate fallback processes are in place for activating services where the electronic system cannot be used to identify a prepaid user.²⁶

Prior to becoming the ACMA, the Australian Communications Authority (ACA) published annual reports that include a brief section on the prepaid Determination and this can be expected to continue into the future. In addition, the ACA’s Law Enforcement Advisory Committee prepared a report in 2002-03 on the topic of identity fraud and prepaid phones for the government’s Joint Standing Committee on Electoral Matters.²⁷

²⁶ *ibid.* (p. 22)

²⁷ This is reported in the ACA Annual Report 2002-03 (p. 65).

To assist mobile operators and consumers to interpret the prepaid Determination, the ACMA has published explanatory statements on its website. These statements serve in place of an industry-wide code of practice for the collection of personal information from prepaid customers. The explanatory statement for mobile operators provides detailed instructions on identity collection requirements for a range of scenarios, for both Part 3 and Part 4 methods.²⁸

Australia maintains a national Integrated Public Number Database (IPND) for emergency service and law enforcement purposes. It is also a shared resource for public number directories and directory assistance services. The IPND contains all listed and unlisted telephone numbers in Australia including fixed line, mobile and satellite services as specified in Part 4 of Schedule 2 in the *Telecommunications Act 1997*. Incumbent operator Telstra is responsible for administering the IPND.

Mobile operators are required to submit details of all prepaid customers to the IPND. It is industry practice to submit details provided during the post sale activation process rather than information collected at point of sale. As noted above, this can in some instances lead to errors and is partly responsible for the relatively low quality of prepaid mobile service records in the IPND.

The regulatory authority's Annual Report contains a section on the IPND, which provides an update on issues and developments associated with it. In the 2002-03 report, for instance, the ACA noted that it had issued a formal warning to a "public number directory producer" for contravention of the industry guidelines pertaining to the use

of the IPND. The ACA's Performance Report for 2002-03 indicated that the IPND contained nearly 50-million records in 2002, with 12 telecommunications companies providing data to it and four authorized commercial users drawing data from it. Commercial data users provide "location dependent carriage services" as well as public directory services.²⁹

The data contained within the IPND may only be accessed for the purposes specified in clause 10 (1) of the *Carrier Licence Conditions Declaration 1997*, which pertains to Telstra's role as database administrator:

... the licensee must establish and maintain an industry-wide integrated public number database to provide information for purposes connected with the following activities:

- providing directory assistance services;
- providing operator services or operator assistance services;
- publishing public number directories;
- providing location dependent carriage services;
- the operation of emergency call service or assisting emergency services ... ;
- assisting enforcement agencies or safeguarding national security ... and
- any other activities specified by the ACA by written notice to the licensee.

In May 2003, a private firm was contracted to undertake an audit of the IPND to determine the accuracy of the data and to assess the procedures and processes associated with the provision of customer records. Findings reported in July 2003 indicated an unacceptable level of errors in the IPND and subsequently prompted the regulatory authority to encourage data providers to improve the quality of records by issuing "report cards" to them. The audit program is to continue annually to 2006.

28 Australian Communications and Media Authority. (no date). Buying a pre-paid mobile phone service? Available http://www.acma.gov.au/ACMAINTER.2490560:STANDARD::pc=PC_1899; Australian Communications and Media Authority. (no date). Explanatory Statement to the Telecommunications (Service Provider - Identity Checks for Pre-paid Mobile Telecommunications Service) Determination 2000. Available http://www.acma.gov.au/ACMAINTER.2490560:STANDARD::pc=PC_330#Outline.

29 Australian Communications Authority. (2003). Telecommunications Performance Report 2002-03. (p. 187).

The IPND is managed according to a detailed set of technical and procedural standards developed and reviewed by the Australian Communications Industry Forum (ACIF) Working Group. Among these standards is the document titled *Industry Code ACIF C555:2000 Integrated Public Number Database (IPND) Data Provider; Data User and IPND Manager*, which provides formal specifications on all matters related to the maintenance of the IPND.


In March 2005, the Australian Privacy Commissioner as part of a wider review process, investigated a number of allegations made against telecommunications providers under section 40 (2) of the *Privacy Act 1988* concerning the use and disclosure of unlisted numbers in the IPND. The review of the Privacy Act included consultations from industry, consumer and privacy groups, charitable organizations and business. The outcome of this review included recommendations to amend both the Privacy Act and Telecommunications Act to specify the use and disclosure of phone numbers, to include small businesses in privacy legislation, and to clarify Part 13 of the Telecommunications Act.³⁰

The ACMA also conducted a consultation in summer 2005 to address perceived problems with the current ACIF code governing the IPND. The ACMA is now considering submissions and working with the Telecommunications Industry Ombudsman, the Office of the Privacy Commissioner and the Consumer Commission to finalize a new industry standard to regulate the use and disclosure of customer data in the IPND.³¹

30 Office of the Privacy Commissioner, Australia. (2005, March). Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988. Retrieved October 11, 2005 from <http://www.privacy.gov.au/act/review/revreport.pdf>.

31 Australian Communications and Media Authority. (2005). Who's got your number? Regulating the Use of Telecommunications Customer Information. Available http://www.acma.gov.au/ACMAINTER.2490560:::pc=PC_2527.

Austria (AT)


 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
3,330 (50.9%)	3,259 (48.4%) ↓	3,338 (47.1%) ↓

Source: OECD (2005) *Communication Outlook*.

A survey response was not received for Austria but informal correspondence indicated that the government of Austria does not require mobile operators to collect customer information when activating prepaid accounts.

Some operators are reported to offer incentives to provide personal details for marketing purposes. One new entrant in the country is also reported to be selling prepaid cards “entirely anonymously” in the discount supermarket chain Hofer/Aldi.

Belgium (BE)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
5,154 (67.0%)	5,331 (65.5%) ↓	5,429 (62.3%) ↓

Source: OECD (2005) *Communication Outlook*.

The government of Belgium does not require mobile operators to collect customer information when activating prepaid service accounts. The government has neither issued a public statement nor sought expert or public opinion on this matter.

The respondent was not able to provide information on any background studies that might support or oppose identity requirement for prepaid service in Belgium.

Mobile phone operators do not publish a code of practice for collecting customer information from prepaid account holders.

Belgium does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement.

Canada (CA)

Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
2,736 (25.7%)	2,937 (24.7%) ↓	3,147 (23.8%) ↓

Source: OECD (2005) *Communication Outlook*

The government of Canada does not require mobile phone operators to collect customer information when activating prepaid service accounts. There has, however, been some pressure exerted by law enforcement to introduce a registration policy. In April 2003 the government published a summary of submissions in response to a Lawful Access consultation, which indicate that law enforcement agencies have called for a prepaid registration policy in Canada:

Pre-paid/pay-as-you-go cellphones, Internet access cards, Internet cafes and Internet facilities at public libraries all pose an obstacle to law enforcement agencies because the identity of the service user is easy to conceal from law enforcement.

In keeping with the principle that no intercept safe havens be created, regulatory obligations should be established in Canada requiring the identification of users of prepaid communications services and the maintenance of an accurate subscriber database by the service provider.³²

There do not appear to be any background studies to support or oppose prepaid registration in Canada but civil society groups have opposed it on principle as a privacy rights issue:

[Communications Service Providers] should not be obliged to collect

32 Nevis Consulting Group. (2003, April 28). Summary of Submissions to the Lawful Access Consultation. Department of Justice Canada, 2004. (p. 18). Available http://www.canada.justice.gc.ca/en/cons/la_al/

subscriber information that they do not already collect in the normal course of their business. This proposed obligation would likely impact most service providers and retailers selling prepaid and other anonymous telephone cards and phones. As noted by the Privacy Commissioner of Canada, this would be a gross invasion of privacy and present significant opportunities for data leakage or loss (and subsequent threats, such as identity theft).³³

For its part, the Canadian Wireless Telecommunications Industry Association also opposed a registration policy on the grounds that it “might cause the elimination of certain services, or class of services, such as prepaid wireless.” The CWTA underscored this point by pointing to the incongruence of an identity requirement for prepaid service:

... [a] problem is created with respect to prepaid wireless services provided by wireless carriers since valid customer information is not required by carriers in order to provide prepaid services. Given that a credit check is not required, and that the customer will never receive a monthly bill, there is no need for the carrier to request the customer’s name or address. The entire transaction of activating the customer’s account can be conducted over the phone and absent any identification. Although wireless carriers are increasingly requesting customer name and address information for business purposes, this information is not validated, nor do carriers deny service if the customer does not provide this information.³⁴

33 *ibid.* (p. 41)

34 Canadian Wireless Telecommunications Association. (2002, Dec. 16). Lawful Access Consultations: Response of the Canadian Wireless Telecommunications Association. (par. 71). Available <http://www.cwta.ca/CWTASite/english/otherfederal.html#>

Canada does not have an integrated public number database (IPND) for the purpose of law enforcement or public safety. During the Lawful Access Consultation the idea of an IPND being developed for Canada was introduced, to which the Privacy Commissioner responded in opposition, criticizing the consultation paper of treating privacy too lightly on this matter:

The paper suggests that it might be appropriate to create a national database containing the customer name and address and service provider information for all Canadian telephone subscribers—as recommended by the Canadian Association of Chiefs of Police.

I cannot support the creation of such a database. Yes, it would make it easier for law enforcement/national security agencies to obtain customer name and address and service provider information, but the difficulties involved in obtaining this information can hardly be insurmountable. Furthermore, these difficulties serve a purpose—they force law enforcement/national security agencies to think twice before seeking to obtain this information.

The consultation paper appears to endorse a view that the name and address of an individual with a given telephone number carries such a low expectation of privacy that access to it by law enforcement authorities should be a routine procedural matter. I take issue with any assertion that one’s name and when associated with a unique identifier like a telephone number, is somehow unworthy of privacy protection.³⁵

35 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

It is unlikely that a prepaid registration requirement will be introduced in Canada as a result of this consultation; however, final determinations stemming from the Lawful Access Consultation remain uncertain.³⁶

Czech Republic (CZ)

Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
3,016 (43.4%)	6,731 (78.2%) ↑	7,268 (74.9%) ↓

Source: OECD (2005) *Communication Outlook*

The government of the Czech Republic does not require mobile phone operators to collect customer information when activating prepaid service accounts. However, the respondent has indicated that the government did discuss the issue in parliament in May 2005. The *Prague Post* newspaper reported on February 24, 2005 that the government’s Chamber of Deputies Security Committee appealed to cabinet on January 27, 2005 to draft a law “to ban anonymous SIM cards.” It appears that this proposal was not put into effect.

A number of government spokespersons are quoted in the *Prague Post* article, including a Security Committee member who stated that “Should a ban come into force, as it has in Germany, Italy, or Great Britain, there would be less need for police wiretapping.” This comment suggests that proponents of the measure see it as an aid to law enforcement but that they might not have been well briefed on its implementation in other countries given that Great Britain has never implemented prepaid regulations.


36 On November 15, 2005 The *Modernization of Investigative Techniques Act (MITA)* was introduced in the Canadian Parliament. This bill (C-74) is concerned with the retention, use and disclosure of subscriber information as it pertains to lawful interception of telecommunications. In its present form it does not require mobile operators to register prepaid customers. See: <http://www.psepc-sppcc.gc.ca/media/nr/2005/nr20051115-en.asp>

The respondent was not aware of any formal study undertaken in the Czech Republic that might support or oppose a prepaid registration policy, although discussions were held at one time between the regulatory authority and the Association of Mobile Network Operators to consider the costs/benefits of prepaid registration. The respondent did not indicate any documentation associated with these discussions. Similarly, there is no evidence to suggest that the government has considered alternative means for identifying prepaid customers.

Mobile phone operators do publish corporate policies regarding collection of customer identification as part of their general terms and conditions of service. The collection of information from prepaid customers is voluntary and at present operators are not seeking to make this a mandatory condition of service provision.

The Czech Republic does not have an Integrated Public Number Database (IPND) for the express purpose of public safety and law enforcement. The incumbent operator (Cesky Telecom) is, however, obligated as the Universal Service Provider in that country to maintain and publish a public directory of telephone numbers for directory assistance purposes. This public directory only contains mobile phone numbers of subscribers who have requested their publication.

Denmark (DK)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
1,474 (37.2%)	1,354 (30.2%) ↓	1,118 (23.5%) ↓

Source: OECD (2005) *Communication Outlook*

The government of Denmark does not require mobile phone operators to collect customer information when activating prepaid service accounts. The government has neither issued


a public statement nor sought expert or public opinion on this matter.

The respondent was not able to provide information on any background studies that might support or oppose identity requirement for prepaid service in Denmark.

The respondent was not able to indicate if mobile phone operators publish a code of practice for collecting customer information from prepaid account holders.

Denmark does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement.


Finland (FI)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
83 (2.0%)	90 (2.0%) ↗	94 (2.0%) ↗

Source: OECD (2005) *Communication Outlook*

Information was not received for Finland.

France (FR)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
18,061 (48.8%)	17,108 (44.3%) ↓	17,146 (41.1%) ↓

Source: OECD (2005) *Communication Outlook*

The government of France requires mobile phone operators to collect information from customers when activating prepaid accounts. The Director of Post and Telecommunications, within the Interior Ministry, issued a letter to all mobile operators in 1997 requesting them to collect and retain information about prepaid customers. The respondent indicated that this letter and request were intended to ensure that prepaid services would fulfil obligations “of the law of

11th of July 1991 about correspondence secrecy and interceptions.”

It is not known if the government of France sought and/or received expert or public opinion concerning identity requirements for prepaid service in conjunction with this letter. Similarly, the respondent was unable to provide information on background studies that support or oppose the identity requirement for prepaid service in France.

Responsibility for administration of this regulation is left up to each mobile phone operator with no apparent requirement to produce a compliance report for the government or other public authorities. There is also no evidence to suggest that measures have been taken by the government to monitor or enforce compliance of the regulation. Likewise, the mobile phone industry does not publish a corporate or industry wide code of practice regarding the collection of customer information for prepaid accounts.

The respondent was unable to specify if the government has sought opinion on alternative means for identifying prepaid subscribers and it is not known if a report is issued on public safety or law enforcement activities that might involve prepaid mobile users.

France does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement. In principle, the requirement for all mobile phone operators to maintain their own databases of customer records for prepaid accounts establishes the conditions needed for the creation of an IPND of prepaid customers. However, this is no evidence to suggest that such a step has yet been considered by the government of France or by the mobile phone industry.

Germany (DE)

Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
31,374 (55.9%)	31,338 (53.0%) ↓	33,307 (51.4%) ↓

Source: OECD (2005) *Communication Outlook*

Mobile phone operators in Germany are required by law to collect and retain customer information for all telephone subscriptions including prepaid service. This requirement was introduced in June 2004 under a new Telecommunications Act. Section 111(1) of the Act establishes this requirement:

Any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or providing telecommunications connections for telephone numbers allocated by other parties is ... to collect, prior to activation, and store without undue delay the telephone numbers, the name and address of the allocation holder, the effective date of the contract, the date of birth in the case of natural persons, and in the case of fixed lines, additionally the address for the line, even if such data are not required for operational purposes; where known, the date of termination of the contract is likewise to be stored.

Section 111(1) further specifies that operators must amend customer records “without undue delay” when receiving notice of changes and attempt to collect, retroactively, any missing data on existing customers if this is deemed “possible at no special effort.” Upon termination of the contractual relationship, operators are required to retain that person’s data for one year, at which time it must then be erased. This section also states that “Compensation for data collection and storage is not paid.”

The Federal Network Agency or Bundesnetzagentur (BNetzA) has been given responsibility for

administering the identification requirements in Section 115 of the new Act. Under Section 115, the Bundesnetzagentur, formerly the Regulatory Authority for Telecommunications and Posts, is authorized “to enter and inspect” business premises and to issue fines to mobile operators not exceeding €20,000 in order to enforce the identity collection obligation under Section 111(1). In certain cases additional powers are provided:

In the event of repeated violations of the provisions of section 111(1) ... the activities of the person with obligations [to collection customer information] may be restricted by order of the Regulatory Authority in such a way that his customer base may not be changed, except as a result of contract expiry or notice of termination, until such time as the obligations ensuing from these provisions have been fulfilled. [Section 115(2)]

In a worst-case scenario, the Bundesnetzagentur has the power to

... wholly or partially prohibit operation of the telecommunications system concerned or commercial provision of the telecommunications service concerned if less severe action to enforce proper conduct is insufficient. [Section 115(3)]

BNetzA has not yet produced a report on compliance with Section 111(1) and it is not known if such a report is planned for future. Similarly it is not known if BNetzA has yet taken action to enforce compliance with any mobile operators in Germany.

The provisions in the new legislation are the result of a compromise between the German parliament and the council of federal states. The idea to introduce mandatory identification for prepaid mobile phone service was first introduced by the Deutsche Bundesrat (council of federal states) in a draft version of the Act in October 2003. This arm of government “is primarily responsible for matters relating to public security

and thus tend[s] to advocate far-reaching powers for law enforcement authorities.”

However, it has been reported that the Deutsche Bundestag (German parliament) rejected this provision, among others, and proposed in March 2004 an “exemption” for prepaid mobile phones. In May 2004 a Mediation Committee presented a compromise that removed this exemption from the legislation. The Committee’s compromise also removed a provision that would have allowed mobile operators to be reimbursed for costs associated with providing customer data to law enforcement authorities. The Bundestag adopted the compromise on 6 May 2004, the Bundesrat on 14 May 2004. The new act came into effect in July 2004.³⁷

It is not known for certain if either the Bundesrat or Bundestag sought expert or public opinion in conjunction with a proposed identity requirement for prepaid mobile phones. Nevertheless, there is some evidence to suggest that the government has not yet benefited from such opinion. On May 24, 2002 in reference to the proposed changes to the Telecommunications Act, Germany’s Data Protection Commissioners issued a joint statement indicating that no research had been done on the question of prepaid registration and its value to law enforcement authorities.³⁸

However, it was reported by the respondent that in 2005 the German regulator BNetzA issued a questionnaire to mobile operators to obtain data on feasibility and potential costs of proposed data retention provisions. It is not known if this survey included questions about prepaid service

37 Background to the German Telecommunications Act of 2004 is reported by European Digital Rights (EDRI) in its *EDRI-gram* news bulletins number 2.10 (19 May 2004) and number 2.5 (11 March 2004). Available online at <http://www.edri.org/>

38 Entschließung der Datenschutzbeauftragten des Bundes und der Länder , “Geplanter Identifikationszwang in der Telekommunikation” [Resolution of the commissioners for data protection of the federation and the countries, “Planned identification obligation in telecommunications”] Statement dated 24 May 2002. Available online at <http://www.lfd.m-v.de/beschlue/ent2002.html#nr.1>

or if a separate questionnaire was issued in relation to prepaid mobile phones, either before or after the new Telecommunications Act came into force.

Similarly, it is not known for certain if the German government has sought and/or received opinion on alternative means for identifying mobile phone customers. This is in contrast to reported use of IMSI-catcher technology in that country. The use of IMSI-catcher technology to intercept mobile phone calls is apparently allowed in the Federal Constitution Protection Law (Section 9.4) and its use has been reported in the German press. Usage of the IMSI-catcher is also regulated in section 100i of the Code of Criminal Procedure (StPO). It was also mentioned in an early draft of the new Telecommunications Act in 2003.

Despite the apparent use of IMSI-catcher and the identification requirements included in the new Telecommunications Act, the German government has not issued any public reports that indicate the cost of these measures to mobile operators or the benefits they are providing for law enforcement and national security authorities.

An inquiry to the German regulator BNetzA yielded no mention of specific background research that might support a prepaid identification policy. However, a study by the Max Planck Institute for Foreign and Criminal Law published in May 2003, did raise the practical problem of differentiating between registered users of mobile phones and the actual user of the phone at any given moment in time. Nonetheless, the overall finding of the study claims that telecommunications surveillance is an “important and indispensable instrument, which has led to the pursuable and fundamental success regarding investigations in specific fields” [respondent’s translation].

By contrast there is some evidence to suggest deliberate efforts by the German government to move ahead with legislation before research was completed. In a statement of June 12, 2002 the Deutsche Bundesrat demanded a “general extension” of telecommunications surveillance, citing problems with crime that

included terrorism, sexual offences, white collar crime, and trafficking in human beings. In that statement the Bundesrat claimed that it could not afford to wait for the results of studies into the effectiveness of telecom surveillance then being undertaken at the time (including the Max Planck study which had not yet been published).

There are a number of studies in Germany that oppose the extension of telecoms surveillance measures, including prepaid registration, on two grounds: constitutionality and cost recovery. Patrick Breyer, a German lawyer, published an extensive report in November 2004 and later filed a document with Federal Constitutional Court on June 20, 2005 that has raised a number of constitutional concerns with regard to the new Telecommunications Act in Germany. These concerns included the obligation of customers to provide personal information in the registration process for prepaid mobile phone service. According to the respondent, Breyer’s document claims that the new regulations are unconstitutional because they are “disproportional” insofar as “a public interest in the investigation and prevention of criminal acts does not [outweigh] private interests.” The respondent listed several arguments provided by Breyer to support this claim, including one that notes a specific problem with the prepaid registration policy:

The common good is not promoted since organized criminals are able to continue the anonymous use of prepaid mobile phones. For example, the use of false identities is not prevented since the Telecommunications Act does not oblige providers to verify any data provided by customers. [Respondent’s comment; question E1]

The respondent also noted that mobile operators have sought to challenge data retention provisions in the new Telecommunications Act on constitutional grounds, but for a slightly different reason:

From the point of view of the [telecommunications service] providers

... the obligation to support public authorities with the implementation of a system to enable remote access to customer data is to be judged as an unequal and therewith unconstitutional treatment compared with other companies that provide communication services which do not have to collect and provide data as for example enterprises that transport mail and offer other postal services. Due to the public interests in the collection and transfer of data, the obligation of providers is seen as an illegitimate tax. [Respondent's comment; question E1]

Along similar lines, industry groups VATM and BITKOM have produced research studies on the associated costs of traffic data retention, arguing the need for appropriate compensation for mobile operators who are required to collect, retain, and disclose this data to law enforcement authorities. While important for other reasons, these studies are not primarily concerned with the specific privacy issue or costs associated with identity collection requirements for prepaid mobile phone service.

Despite the identity collection requirements in the new Telecommunications Act, there does not (yet) appear to be a common industry code of practice or agreed best practices for the collection, storage, or transfer of customer data to requesting authorities. General specifications for the contents of "customer data files" and for the method of data transfer are established in Section 112 of the Act, and the right of the government to establish specific technical procedures for data retrieval and transfer is established in Section 112(3). It appears to be the case that the Act assigns the Bundesnetzagentur (BNetzA) an intermediary role in the retrieval and transfer procedures between requesting authorities and mobile operators:

The Regulatory Authority can, at all times, retrieve from customer files data for information requests from the authorities referred to in subsection (2)


by means of automated procedures in the Federal Republic of Germany.

Authorities that are granted right of access to customer data files are specified in Section 112(2):

- Courts and criminal prosecution authorities
- Federal and state police "for the purposes of averting danger"
- Customs Criminological Office
- National security agencies (Federal Armed Forces, Counter-Intelligence Office, and Federal Intelligence Office)
- Emergency service centres
- Federal Financial Supervisory Authority
- Authorities responsible for the prosecution of offences related to the Undeclared Work Act

The new Telecommunications Act does not establish a standalone Integrated Public Number Database (IPND), although the combined customer databases of mobile operators in Germany should, at least in principle, serve as a *de facto* IPND for requesting authorities. As such, the technical and legal procedures described in Section 112 of the Act, provide a basis for the administration of this collective database. A statement of requirements for public reporting of compliance issues and/or cost/benefit assessments of the Act's provisions under Section 111 and 112 are not apparent in the new Telecommunications Act, although this has not been confirmed for this study.

Greece (GR)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
5,029 (63.1%)	6,066 (65.1%) ↑	6,757 (65.4%) ↑

Source: OECD (2005) *Communication Outlook*

The government of Greece does not require mobile phone operators to collect customer information when activating prepaid service accounts. The respondent indicated that Hellenic law 2774/1999 for the protection of personal

data establishes a statutory basis that prohibits collection of personal data from customers using prepaid cards, should those customers choose to remain anonymous. However, in cases where customers elect to provide personal details to a mobile operator, the Hellenic Data Protection Authority has issued a decision that obliges those operators to verify those details through an identity check and to ensure that customer records are accurate and up to date.

The government has not received expert or public opinion concerning the introduction of identity requirements for prepaid customers; however, the respondent stated that the Hellenic Data Protection Authority drew attention to and opposed a prepaid registration requirement in the draft bill for transposition of EU Directive 2002/58/EC.

The Greek government has neither sought opinion on alternative means of identifying mobile phone customers, nor does it produce a report on law enforcement activities that might include details about prepaid customers.

In spite of data protection requirements to verify customer identity when collecting personal details, it is not known if mobile operators in Greece have developed either individual corporate policies or an industry-wide code of practice regarding data collection procedures. Similarly, the respondent did not indicate if the Data Protection Authority has published procedural requirements for the collection of personal details from prepaid mobile phone customers.

Greece does not maintain an Integrated Public Number Database (IPND) expressly for the purpose of law enforcement or public safety.

Hungary (HU)

Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
3,584 (72.2%)	5,378 (78.1%) ↑	6,157 (77.5%) ↓

Source: OECD (2005) *Communication Outlook*

The government of Hungary requires mobile phone operators to collect information from customers when activating prepaid and post-paid accounts. This requirement is set out in the Electronic Communications Act (Act C of 2003), which stipulates that customers must identify themselves at point of sale when purchasing prepaid phones. Article 129 (6) in Act C of 2003 describes the information required to establish an individual subscriber contract:

The individual subscriber contract concluded in writing shall contain at least the following provided that the specific features of the service make this possible:

[...]

- b) name, residence, place of stay or seat of the subscriber;
- c) in the case of a natural person subscriber, the name (maiden name) of the subscriber, his/her mother's name, and place and date of birth;
- d) in the case of a subscriber that is not a natural person, the trade registry number or other registration number of the subscriber and its bank account number;

Article 157 (2) indicates that service providers are obliged to collect details of the mobile phone SIM card and the IMEI (International Mobile Equipment Identification) number for each prepaid customer.

It is not known if the government of Hungary has sought or otherwise received expert or public opinion concerning the introduction of this requirement. Similarly, the respondent was not able to indicate if the government sought opinion


on alternative means of identifying mobile phone customers or if the government produces or makes available a report on law enforcement activities that might include details about prepaid users.

The respondent was not aware of background studies that either support or oppose the prepaid requirement; however, it was suggested that privacy complaints related to prepaid service would be filed with the Data Protection Officers who are responsible for internal data protection of organizations. The Office of the Parliamentary Commissioner for Data Protection and Freedom of Information is the general authority for enforcing rights to the protection of personal data. The Commissioner of this office is elected by Parliament and is able to operate independently. It is not known if any complaints have in fact been submitted to this office. However, during the last ten years, many inspections by the Commissioner in telecommunications revealed many incidences of illegitimate data handling at mobile service providers, including the use of subscriber data in direct marketing, copying documents and data collection, among others.

There is no industry-wide code of practice for the collection of subscriber information from prepaid customers. The Hungarian Communications Authority and Ministry of Informatics and Communications were listed as government authorities designated to administer the identity requirements for prepaid service in Hungary. There is a provision in Act C of 2003 under 151 (3) that allows the Hungarian Communications Authority to enforce compliance through fines, however, it is not known if these measures have been used.

Hungary does not maintain an Integrated Public Number Database (IPND) for the express purpose of law enforcement or public safety.

Iceland (IS)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
88 (37.4%)	88 (33.7%) ↓	112 (40.3%) ↑

Source: OECD (2005) *Communication Outlook*

Information was not received for Iceland.

Ireland (IE)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
1,967 (71.0%)	2,210 (71.8%) ↑	2,510 (73.4%) ↑

Source: OECD (2005) *Communication Outlook*

The government of Ireland does not require mobile operators to collect customer information when activating prepaid accounts. The Irish government did consider a national register for 3G mobile phones as a measure to protect minors from harmful content. Following strong lobbying from the mobile phone industry, the government accepted technical proposals from the industry in November 2004 as an alternative to a national register.

Aside from the lobbying efforts of industry it is not known if there are any background studies produced by any organization that explicitly support or oppose an identity requirement for prepaid services in Ireland.


The respondent indicated that some mobile operators offer customers a €70 call credit if they register their details online, but this a voluntary measure for commercial purposes only.

In June 2004, the Irish Cellular Industry Association published a code of practice intended to promote the safe and responsible use of mobile phones, particularly among minors. The code of practice does not cover the collection of customer information but is instead concerned

with the use and disclosure of customer records. In particular, the respondent indicated that “it will allow operators to grant parents authorized access to their children’s prepaid mobile phone records and account details, so they can check what numbers have been called and what services have been accessed.”

The government of Ireland does not maintain an integrated public number database (IPND) expressly for the purpose of public safety and law enforcement.

Italy (IT)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
45,792 (89.6%)	47,732 (89.9%) ↑	51,705 (91.2%) ↑

Source: OECD (2005) *Communication Outlook*

A survey response was not received for Italy but recent news reports indicate that the government issued a decree on 27 July 2005 under its data retention legislation that has introduced compulsory identification for mobile telephones. The European Digital Rights bulletin *EDRI-gram* published details of the policy in August 2005:

Resellers of mobile subscriptions or prepaid cards must take all measures to guarantee the identity of [the] purchaser and keep a photocopy of each presented identity card. Article 7 decrees that all internet cafes and public telephone shops with at least 3 terminals must seek a license permit within 30 days from ‘questore,’ a local representative of the Ministry of Home Affairs. ... WIFI-points and locations that do not store traffic data will have to preventatively demand ID from their users. This actually already is common practice in Italy; hotspots at several airports for example will only allow internet usage after the

user has entered the serial number of his ID card or drivers license.³⁹

EDRI reports that this requirement is a subject of intense debate in Italy because of the high costs of compliance but further details are not known about the registration policy.

Japan (JP)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
1,847 (2.5%)	2,084 (2.6%) ↑	2,609 (3.0%) ↑

Source: OECD (2005) *Communication Outlook*

The government of Japan requires mobile phone operators to collect information from customers when activating prepaid accounts. The registration requirements follow in the wake of concerns about phone scams known as “It’s me!” cases in 2004. The Ministry of Information and Communications (MIC) introduced new measures “to reinforce personal identity” with prepaid services and the government has passed legislation to control the sale and resale of prepaid phones. According to an MIC report published in 2005,

... the Law on Confirmation of Personal Identification of the Subscribers, etc. by Voice Mobile Communications Carriers and Prevention of Misuse of Voice Mobile Communications Services was proposed to the 162nd session of the Diet as a bill presented by a Diet member, and the bill was approved in April 2005. This law punishes acts including the following: an act of declaring a false name or address upon subscription, etc.; an act of commercially transferring mobile phones or PHS [Personal Handyphone System] to others for value without the consent

39 Italy decrees data retention until 31 December 2007. (2005, Aug. 10). EDRI-Gram 3.16. Retrieved October, 2005. Available <http://www.edri.org/edriagram/number3.16/Italy>

of the mobile phone/PHS carriers; an act of commercially lending mobile phones/PHS to others for value without confirming the name and address of the borrower; an act of transferring mobile phones/PHS owned by others.⁴⁰

The registration requirement in Japan came into effect in April 2005 and all customers were required to register their prepaid mobile phones with their carrier by October 31, 2005. Customers not registered by the deadline would have their service suspended. It is not clear if the carriers are required to report to the government on the number of suspensions that have taken place after the deadline passed.

Two public hearings were held in 2004 (November 4, 16) to bring mobile operators and consumer groups together with the government to discuss the problem of telephone fraud, including the role of prepaid services in such cases. Opinions voiced at the hearings may have played a role in the government decision to abandon an initial proposal that would have placed an outright ban on prepaid mobile phone service in that country. News reports indicate that this proposal, which was tabled by the government in October 2004, received considerable opposition from mobile carriers and from Japan's European Business Community, which called it a "disproportionate response" to the problem.⁴¹ At the time, Japan's largest mobile operator, NTT DoCoMo, declared it would stop selling prepaid phone service altogether, its president stating at a press conference that "DoCoMo considers prepaid phones unnecessary as they involve

various social problem."⁴² It is not known if NTT DoCoMo has acted on this declaration in light of the registration policy that has replaced the proposed ban.

Despite public opposition to the proposed ban and the high profile of the prepaid issue in Japan, the respondent was not able to provide information about any specific research studies that either support or oppose an identity requirement for prepaid service.

With the registration policy now in effect, customers are obliged to provide their personal details and identification not only at the time of initial activation but also when a prepaid phone is acquired from a third party through a private transfer. In such cases, the law requires that both customers contact the mobile operator to report the details of the transfer. Mobile operator Vodafone describes four distinct cases to help its customers understand the requirements:

- **No registration:** You did not register your customer information at time of purchase.
- **Change of address:** You registered your customer information at the time of purchase, but later changed your address.
- **User change:** You received a prepaid mobile phone from the person whose customer information was originally registered at the time of purchase.
- **No longer in service:** You registered your customer information at the time of purchase, but later gave the prepaid mobile phone away.

In the first two cases the current user of the prepaid mobile phone must visit a retail outlet with proof of identity to register or update their customer information with the operator. In the latter two cases, *both the previous and the current user* of the prepaid mobile phone must visit a retail outlet with proof of identity to update

40 Japan Ministry of Internal Affairs and Communications. (2005). Information and Communications in Japan: Stirrings of u-Japan. 2005. (p. 63). Available <http://www.johotsusintokei.soumu.go.jp/english/>

41 European business slams Japan's plan to ban prepaid cell phones. (2004, Nov. 10). Japan Today. Retrieved Dec. 21, 2004. Available <http://www.japantoday.com/e/?content=news&cat=4&id=318374>

42 DoCoMo to stop offering prepaid cell phone services. (2004, Oct. 1). Japan Today. Retrieved Oct. 26, 2004. Available <http://www.japantoday.com/e/?content=news&cat=4&id=313920>

the customer information associated with that phone.⁴³ Annex C contains a sample customer notification document.


The “It’s me!” scam involves elderly Japanese being contacted by strangers, often using prepaid mobile phones to disguise their identity. One news source indicates that over ninety per cent of cases involved a prepaid phone, although a source is not given for this claim.⁴⁴ In these cases, the perpetrator pretends to be a relative in distress, who is in need of some quick cash and asks that money be transferred into a phoney bank account.

Records from the Japanese National Police Agency indicate a drop in incidents of reported “It’s me!” cases after the prepaid registration policy came into effect but this may also be related to independent police initiatives, such as a special task force that was established in late 2004 to deal with rising incidents of telephone fraud.⁴⁵

It is not known if either the Ministry of Information and Communications or the National Police Agency in Japan will produce a report on compliance with the registration requirements. Similarly, it is not known if any legal action has been taken to enforce compliance, but the legislation does permit the government to issue fines and prison terms for failure to comply with the regulations, although it is not clear to what extent mobile carriers are liable in cases of non-compliance.

The government of Japan does not maintain an Integrated Public Number Database (IPND). It is not known under what terms and conditions mobile operators are required to make their records of prepaid customers available to the government.


Korea (KR)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
n/a	607 (1.9%)	591 (1.8%) ↓

Source: OECD (2005) *Communication Outlook*

Information was not received for Korea.


Luxembourg (LE)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
179 (41.5%)	179 (37.9%) ↓	318 (59.0%) ↑

Source: OECD (2005) *Communication Outlook*

Information was not received for Luxembourg.

Mexico (MX)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
19,974 (91.8%)	23,922 (92.3%) ↑	28,069 (93.3%) ↑

Source: OECD (2005) *Communication Outlook*

The government of Mexico does not require mobile phone operators to collect customer information when activating prepaid service accounts. The respondent was uncertain if the government had either issued a public statement or sought expert or public opinion on this matter.

The respondent was not able to provide information on any background studies that

43 The Vodafone Japan website provides customers with information about registering their details when purchasing a prepaid mobile phone. Available: <http://www.vodafone.jp/english/products/index.html>

44 Japan rejects ban on prepaid mobiles. (2004, Nov. 16). *Telecomasia.net*. Retrieved Dec. 21, 2004. Available <http://www.telecomasia.net/telecomasia/article/articleDetail.jsp?id=133526>

45 Terrorist tracking center planned. (2004, Dec. 14). *Japan Times*. Retrieved October, 2005. Available <http://search.japantimes.co.jp/print/news/nn12-2004/nn20041214f2.htm>

might support or oppose identity requirement for prepaid service in Mexico.

The respondent indicated that mobile phone operators do not publish a code of practice for collecting customer information from prepaid account holders.

Mexico does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement.

Netherlands (NL)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
7,500 (65.2%)	7,400 (62.7%) ↓	8,100 (61.8%) ↓

Source: OECD (2005) *Communication Outlook*

The government of the Netherlands does not require mobile phone operators to collect customer information when activating prepaid service accounts. However, when prepaid cards were first introduced in that country (c. 1997) the Ministry of Internal Affairs is purported to have proposed a ban on anonymous ownership to which the data protection authority (College Bescherming Persoonsgegevens) was opposed.

According to the respondent, an event was organized by a mobile operator in the Netherlands for law enforcement authorities to demonstrate the effectiveness of alternative means of identifying mobile phone users:

When prepaid was introduced, registration of users was discussed. Mobile operators themselves persuaded authorities (and law enforcement) not to introduce this obligation. [The mobile operator] invited some people (Justice, police) and showed them that if [it] was given two dates, periods and two places where somebody was seen calling, [the operator] could find the number calling ... When this was proven, the discussion about registration ended. (Even though

this doesn't say anything about the identity of the user). [Response to question A4]

Despite this apparent rejection of a registration requirement, the European Digital Rights group EDRI reported in December 2004 that the government of the Netherlands requires operators of prepaid mobile phones to store location data for a period of three months.⁴⁶ However, this statement has not been verified.

The government does not publish a report on law enforcement or national security activities that might include information about prepaid phone users.

It is uncertain whether any background studies have been done that either support or oppose prepaid registration policy. The respondent suggested that the data protection authority (mentioned above) might have issued a public statement in its opposition to any such proposal.

There is no industry-wide code of practice regarding the collection of customer information from prepaid mobile phone subscribers in the Netherlands. At least one mobile operator offers an incentive to its prepaid customers to provide their details in exchange for a "top-up" bonus. The use and disclosure of these details is governed by existing data protection laws in the country and used for direct marketing activities.

The Netherlands does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement. However, the respondent stated that mobile operators are obliged to provide access to their customer databases for law enforcement purposes:

We ... do have a database with details of all our subscribers and we do provide that information to law enforcement

46 European Digital Rights. (2004). Bitkom research: no grounds for data retention. EDRI-gram 2.24. Available <http://www.edri.org/edriagram/number2.24/retention>

agencies. Actually we copy our database into a black box and the law enforcement agencies send their requests to that black box/database. This is an automated process using a third party. The legal aspects of this system are still discussed. ... there is a lot of discussion about 'who is the controller of the data in the black box database.' Operators themselves can not access or look into the box. [Response to question D1]

According to the respondent, the situation in the Netherlands "has the same result" as an IPND because law enforcement and other authorized agencies can send requests to several databases to establish a profile or look for a specific individual. The database administrator is purported to issue a report "every now and then" about the use of the databases. It is not known, however, if any form of measure is applied to assess the social value or provide a cost/benefit analysis of this system.

New Zealand (NZ)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
1,661 (68.6%)	1,737 (68.4%) ↓	2,061 (69.7%) ↑

Source: OECD (2005) *Communication Outlook*

The government of New Zealand does not require mobile phone operators to collect customer information when activating prepaid service accounts. A public statement from the government announced they have no plans to tighten controls on prepaid mobile phones⁴⁷. However, the government has not sought expert or public opinion on this matter.

The respondent was not able to provide information on any background studies that

might support or oppose identity requirement for prepaid service in New Zealand.

The respondent was not able to indicate if mobile phone operators publish a code of practice for collecting customer information from prepaid account holders.

New Zealand does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement.

Norway (NO)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
1,649 (43.8%)	1,774 (45.4%) ↑	1,769 (42.5%) ↓

Source: OECD (2005) *Communication Outlook*

As of February 1, 2005 the government of Norway has required all providers of telephone services to collect information from new customers when activating accounts, including those for prepaid service. Existing customers were to be registered by August 1, 2005. After this deadline any unregistered prepaid phones or SIM cards were to be deactivated. It is not known how many deactivations have taken place since this time.

The registration requirement is contained within new Regulations on Electronic Communications Networks and Services (*Ekom Regulations*) enacted on February 16, 2004. Section 6-2 of the Regulations establishes a general requirement for the collection of customer information for all types of telephone service:

Providers of public telephone services shall keep a list of each end-user's name, address and number/address for services requested. The list shall contain information that enables the clear identification of those registered.

Section 6-3 of the Regulations provides a list of identity traits to be collected for each end-user:

47 Govt Says No To Tougher Prepaid Laws. (2006, March 11). The Press. Retrieved March 15, 2006 from <http://www.newsquest.co.nz>.

1. unique ID: date of birth, personal identification number or organisation number, where this is recorded and unless otherwise agreed, or another self-defined unique ID number
2. surname/company name; where the legal owner of a subscription and the user are not the same, only the user's name shall be transferred
3. first name
4. middle name
5. street name or postal address
6. house number
7. postal code,
8. postal town,
9. telephone number
10. user type: i.e. whether the number is used for a fixed-line telephone, mobile telephone, or fax.

Additionally, section 6-2 states that

Providers of public telephone services shall free of charge and *before listing takes place* inform end-users about the purpose of publicly available printed or electronic directories in which information about the end-user will appear and of *the possible use* of the information as a result of the search capabilities of electronic directories. [emphasis added]

This disclosure requirement is notable for two reasons. Firstly because the requirement to inform end-users “before listing takes place” suggests that operators are obliged to tell customers at the point of sale, either through the wording in a contract or by word of mouth, about the reasons for collecting their personal information. The respondent to the survey indicated that there is no industry-wide code of practice published for this kind of procedure, but that at least one operator (Telenor) does include information about registration procedures in its subscription agreement. However, the document provided to validate this claim pre-dates enactment of the 2004 legislation.

The Regulation's disclosure requirement is also notable because it refers to “the possible use”

of customer information, which might include law enforcement and other national security activities. However, the wording of section 6-2 does not refer to law enforcement or public safety, but is rather more concerned with the collection and use of end-user information to support public directory enquiry services.

The respondent indicated that the Norwegian Data Protection Authority was “surprised” by section 6-2 of the Regulations and issued an opinion to challenge it. In conjunction with this challenge, the Data Protection Authority apparently asked for a public debate on the issue by the Norwegian government but this has not taken place. The government of Norway did receive a number of opinions concerning the identification requirement in the new regulations. These documents include the opinion filed by the Data Inspectorate, by mobile operator Netcom, received by the government in September 2003. Details of the opinion are not principally related to the collection of information for prepaid service and instead address a wider set of concerns related to use, disclosure, and retention of personal data.

On 25 August 2004, the regulatory authority and other stakeholder groups met to discuss section 6-2 of the legislation, particularly as it pertained to prepaid service. In a follow-up letter dated 29 September, the regulator presented its proposed set of requirements for the registration of prepaid customers. These were (1) to obtain information “which makes unambiguous identification of the registered users possible;” (2) to ensure that “the information registered at the time of registration [is] of a certain quality;” (3) that any customer “should not be able to use the telephone until the registration is complete.”⁴⁸

Mobile operators Netcom and Sense expressed some concern with respect to this initial set of requirements. This was summarized in a subsequent letter issued by the Norwegian Post

⁴⁸ Annex D contains a copy of this letter translated into English.

and Telecommunications Authority (NPT) to the mobile operators on 8 November 2004:

Netcom and Sense have raised objections ... to the requirement that a mobile phone would not be enabled for use until the user has been unambiguously identified. The companies feel that in order to be able to meet this requirement a 24-hour customer service centre will have to be established, and this would be both expensive and time-consuming. The companies therefore propose that it should still be possible to use the telephone for a limited period before the user is unambiguously identified. [translation]

With respect to the unambiguous identification requirement, NPT had determined in the September letter that “the end-user’s name, date of birth and address will in nearly all cases be sufficient to identify a particular person.” This determination alleviated concerns about the need for mobile operators to collect personal identification numbers from customers, a point which had previously concerned the Data Inspectorate. With regard to the quality assurance requirement, the NPT was asked by law enforcement authorities to consider strict requirements based on Norway’s Money Laundering Act (*Hvitvaskingsloven*) that would oblige mobile operators to conduct face-to-face identity checks with customers when activating prepaid service. It was this interpretation that appears to have prompted the mobile operators’ concern about 24-hour customer service centres.

In response, the NPT determined in the November letter that such a strict requirement was not warranted and that it would be impractical with prepaid service. Instead, the regulator stated its preference for an alternative validation procedure:

A minimum requirement for quality assurance is, however, that the registered information is checked against information in the national population

register (*Folkeregisteret*). Applications for online permission or other permission can be sent to the Central Office for Population Registration (*Sendtralkontoret for Folkeregistrering*). As an equivalent check for customers who are foreign nationals would not be possible, NPT will at a later stage give further consideration to the registration of these customers if there proves to be a large number of false registrations. [translation]

The regulatory authority in this letter also indicated that mobile operators would also be held responsible for the accuracy of their existing customer records, implying that a monitoring and compliance program would be established:

For the sake of good order, NPT would like to remind providers that they also have a responsibility to ensure that the information they hold on existing customers is correct in relation to the demand for unambiguous identification. NPT has legal authority to set further demands pursuant to the provision of paragraph 10-6 of the *Ekom Act* if we learn of false registrations. [translation]

The *Ekom Regulations*, to which these determinations referred, are drawn on the basis of a new Electronic Communications Act (*ekomloven*) that entered into force in July 2003. Under “General Provisions” section 2.8 of the Act requires that

Providers of electronic communication networks that are used for public electronic communications services and providers of such services shall operate networks and services so that statutory access to information on end users and electronic communications is assured.

The provider’s running costs connected with fulfilling this operating duty will be met by the state in regard to those additional costs resulting from these services.

What is notable about section 2.8 of the Act, quoted above, is that it does not make a distinction between various types of telephone service (prepaid/postpaid) or, for that matter, between electronic communications of any kind. Presumably it could therefore encompass all types of electronic communications, including Internet telephony and other forms of data transmission. As such, section 2.8 might provide the basis for regulations that called for any type of electronic communications device to be registered with end-user information. However, it should be stressed here that it is not clear as to whether this is an accurate interpretation of this section, or whether the government of Norway has considered such broad sweeping regulations.

Despite the public hearing held in conjunction with passage of the new Act and the new Regulations, the respondent to the survey could not identify any background studies that explicitly support or oppose an identity requirement for prepaid mobile phone service. It should be emphasized, however, that the legislation and regulations do not specifically mention prepaid services. Nonetheless, a media report in Norway's *Aftenposten* from May 30, 2003 quotes Inger Marie Sunde, chief public prosecutor of the Norwegian Economic Crime Unit *Økokrim*, stating that the presence of unregistered or falsely registered prepaid phones "is a dream situation for certain criminal circles and we have a great number of cases where it has emerged that organized criminals use mobile phones which are impossible to track back to their user." Similarly, in the December 8, 2004 edition of *Aftenposten*, Agder police chief Arne Pedersen is quoted as saying "The use of cash cards by criminals allows them to remain anonymous to police. This often creates problems with police efforts to solve serious crimes." These statements would suggest that some evidence is available to support a prepaid registration requirement, but the respondent to this survey was unable to locate any documented sources that might validate these claims.

The respondent indicated that the government does issue a report on law enforcement activities that might include information on prepaid phone users. However, this response was a slight misinterpretation of the question and referred to a document circulated by law enforcement agencies on November 4, 2003 about the potential impact of international cybercrime initiatives on Norwegian law. Apparently mobile phone registration is mentioned in the document but no specific opinion is stated.

Norway does not have an Integrated Public Number Database (IPND) expressly for the purpose of public safety or law enforcement. It is not clear whether data gathered from individual mobile operators might be aggregated by the regulatory Authority or other government agency for this purpose.

Poland (PL)

Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
5,120 (47.6%)	7,375 (53.1%) ↑	9,467 (54.4%) ↑

Source: OECD (2005) *Communication Outlook*

The government of Poland does not require mobile phone operators to collect customer information when activating prepaid service accounts. The respondent indicated that a proposal to introduce a registration requirement was put forward several times by the Ministry of Internal Affairs and Administration, Internal Security Agency, and the Ministry of National Defense. The Polish Ministry of Infrastructure issued a public statement on May 31, 2004 in conjunction with its proposed changes to the Telecommunications Act:

It was argued that appropriate provisions in question should be introduced for the purpose of prevention and counteracting terrorism and organized crime. However, mobile phone operators expressed their opposition to those solutions which would result in considerable financial

costs on their part. [Response to question E1]

Another criticism of the proposal was that its wording was so vague as to potentially oblige Polish internet portal-sites to register the identities of their free email users. The European Digital Rights newsletter *EDRI-gram* cites a Reuters news report from May 31, 2004 (“Polish Web Portals Criticise Draft telecoms Law”) that describes this opposition to the proposals.⁴⁹


The proposed regulation was removed from the final version of Telecommunications Law that was adopted by the government on 16 July 2004.

It is not known if the government has sought alternative means for identifying prepaid users or if the government issues a report on law enforcement activities that might include information about prepaid users.

It is not known if there are any background studies that either support or oppose a prepaid registration policy in Poland and there is no industry-wide code of practice for the voluntary collection of prepaid customer details.

Poland does not maintain an integrated public number database (IPND) for the express purpose of law enforcement or public safety.

Portugal (PT)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
6,366 (79.8%)	6,690 (78.4%) ↓	7,354 (78.7%) ↑

Source: OECD (2005) *Communication Outlook*

The government of Portugal does not require mobile phone operators to collect customer information when activating prepaid service


accounts. The government has neither issued a public statement nor sought expert or public opinion on this matter.

The respondent was not able to provide information on any background studies that might support or oppose identity requirement for prepaid service in Portugal.

The respondent was not able to indicate if mobile phone operators publish a code of practice for collecting customer information from prepaid account holders.

Portugal does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement.

Slovak Republic (SK)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
1,536 (71.5%)	1,961 (67.1%) ↓	2,284 (62.1%) ↓

Source: OECD (2005) *Communication Outlook*

The government of the Slovak Republic requires the identification of all telephone subscribers, including those with prepaid service. Section 42(3) of the Electronic Communications Act of December 3, 2003 establishes this requirement:

[The mobile operator is obliged to] keep a register of personal data ... of all subscribers of its network, including the subscribers of pre-paid services, in case a user is assigned a telephone number on buying such a service.

Section 55(1) of the Act sets out information that qualifies for data protection and which presumably must be collected by mobile operators under Section 42(3) for all prepaid customers:

... name, surname, academic degree, and address in case of a natural person or business name and seat in case of a legal entity or business name and place

49 Polish proposal to demand ID for pre-paid cards. (2004, June 2). European Digital Rights: EDRI-gram. Available <http://www.edri.org/edriagram/number2.11/prepaid>

of business in case of an entrepreneur— natural person, telephone number, if it should remain private on the request of the user and category of access to the network; data published in the directories of subscribers are not subject to telecommunications privacy.

The respondent indicated that all customers of mobile operators must provide “basic ID from their personal ID card [*obciansky preukaz*] or from a valid international passport.” These details are retained by the mobile operator and disclosed to law enforcement authorities when requested through formal procedures. This requirement is found in Section 57(2) of the Act:

The undertaking providing networks, services or networks and services shall be entitled to obtain and process personal data of users, which include, besides data referred to in Section 55, Subsection 1, Letter b) also the birth registration number, ID card number or number of a different identity proof and nationality, only for the purposes of:

- a) concluding, performance, change or termination of the contract,
- b) billing and registration of receivables,
- c) elaboration of directories of subscribers,
- d) provision of information within activities of co-ordination and operation centres of emergency calls,
- e) co-operation and provision of collaboration pursuant to [law enforcement purposes set out in] Section 55, Subsection 6.

Section 55(6) in turn, establishes the disclosure requirements in relation to Slovak law enforcement authorities:

The undertaking shall be obliged to:

- a) co-operate with the Police Corps and other authorities active in criminal proceedings in investigation of malicious calls and of disseminating alarming information ...
- b) provide necessary co-operation to courts, prosecutors and other state

administration authorities pursuant to special regulations and provide them free of charge, on the base of a written request and in line with the respective regulations, with information, which is subject to telecommunications privacy or to which protection of personal data applies, if the provision of the information or data is necessary for fulfilment of particular tasks of these bodies under the Act;

Having collected this information, mobile operators are obliged to conform to data protection requirements of the Slovak Republic, which are harmonized with relevant EU Directives. As such, the respondent indicated that industry “codes of practice are not necessary from the data protection point of view” because “the law is clear enough and binding enough.” However, this comment seems to pertain to the use and disclosure of customer data rather than with the initial collection at the point of sale.

Section 57(5) of the Act requires that mobile operators “inform the subscriber about what personal data shall be obtained and processed, on the basis of what legal document, for what purpose and for how long the data will be processed.” However, the respondent did not specify if mobile operators in the Slovak Republic have discussed or established a model procedure for informing customers of the rights and responsibilities associated with the actual *collection* of personal details for prepaid service. Similarly, it is not known if the mobile operators are obliged to produce regular reports on compliance with the identity requirement or if the government has ever taken action to enforce compliance.

Section 57(3) of the Act indicates that customer records must be destroyed after termination of the contract, although it is uncertain how this is to be determined in the case of prepaid accounts where such termination may not be immediately apparent to a mobile operator. Also uncertain in this case is the responsibility of mobile operators to erase or update customer records with respect

to the transfer of ownership of a prepaid phone or SIM card. The section is also somewhat ambiguous with respect to certain exceptions to the erasure requirement, particularly in terms of law enforcement or public safety purposes:


The undertaking shall erase personal data without delay upon termination of contractual relations. Exceptions are possible only for the purposes of billing or entering of payments, registration, and enforcement of receivables of the undertaking for the provided service, for handling of users' requests *or in order to comply with other legal obligations and to exercise rights.* [emphasis added]

It is not known if the government has sought or otherwise received opinion regarding the prepaid registration policy in the Slovak Republic. Similarly, the respondent was unable to specify any public documents that would point to specific background studies that either support or oppose the requirement.

The respondent did suggest “there is a very high probability” that law enforcement authorities have alternative means at their disposal for identifying prepaid users, but also indicated that the government has not sought opinion on this matter. It is not known if the law enforcement authorities make available a report on activities that might include users of prepaid services.

The Slovak Republic does not maintain an Integrated Public Number Database (IPND) for the express purpose of law enforcement or public safety.

South Africa (non-OECD)⁵⁰

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
n/a	n/a	n/a

The government of South Africa requires mobile phone operators to collect information from customers when activating prepaid accounts. Prepaid registration falls under Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002. It is not known if expert or public opinion was sought concerning the introduction of the policy. The respondent is unable to provide information about government studies in relation to a prepaid registration policy or alternative means of identifying prepaid customers.

Chapter 7 of the Act sets out the requirements:

- 40.(1) Before any person sells or in any other manner provides, any cellular phone or SIM-card to any other person, he or she—
- (a) must, if the receiver of that cellular phone or SIM-card is a natural person—
 - (i) obtain from him or her—
 - (aa) his or her full names, identity number, residential and business or postal address, whichever is applicable; and
 - (bb) a certified photocopy of his or her identification document on which his or her photo, full names and identity number, whichever is applicable appear;
 - (ii) retain the photocopy obtained in terms of subparagraph (i)(bb); and
 - (iii) verify the photo, full names and identity number. whichever is applicable, of

50 South Africa is a non-OECD country and was not included in the original sample frame for the study. However, contact with a representative from the mobile industry in that country has provided details about its prepaid registration policy, which were deemed relevant to the report.

that person with reference to his or her identification document ...

[...]

- (c) may obtain from the receiver of that cellular phone or SIM-card any other information which the person who sells or in any other manner provides the cellular phone or SIM-card deems necessary for purposes of the Act.
- (2) A person referred to in subsection (1) must ensure that proper records are kept of—
 - (a) the information, including the photocopies, referred to in subsection (1) and, where applicable, any change in such information which is brought to his or her attention;
 - (b) the cellular telephone number or any other number allocated to the other person;
 - (c) the number of the cellular phone concerned; and
 - (d) any other information in respect of the other person which the person concerned may require in order to enable him or her to identify that other person.

Other provisions in the Act include a requirement for customers to report any loss, theft, or destruction of their mobile phone to the police. In addition, persons who are found with a mobile phone and unable to give “a satisfactory account of such possession” may, if there is reasonable suspicion, may be charged with possessing stolen property.

The wording of the Act creates potential problems for administering and enforcing the registration policy, as the respondent indicates:

[The] Act proposes a paper-based collection and retention of certified identity documents by each person that sells or otherwise provides a SIM or handset. Due to extensive use of informal distribution channels, mobile operators are proposing an electronic registration process of storing data in a centralized database [under the control


of] each operator. [Response to question E1]

Despite the difficulties and cost associated with managing such a decentralized registration policy, the respondent was not able to identify any studies that explicitly opposed the requirement. Furthermore, mobile operators and retailers have not published a corporate or industry-wide code of practice on the collection of customer information that might standardize or streamline the procedure.

The government does not make available a report on law enforcement activities that might include prepaid users. The government does not produce a report on compliance with the requirements and it is not known if any action has been taken to enforce compliance.

South Africa does not maintain an Integrated Public Number Database (IPND) expressly for the purpose of law enforcement or public safety purposes. It is not known on what terms and conditions the government is permitted access to the records of prepaid users held by retailers or mobile operators.

Spain (ES)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
19,171 (65%)	21,122 (63.0%) ↓	21,894 (58.4%) ↓

Source: OECD (2005) *Communication Outlook*

The government of Spain does not require the registration of prepaid mobile phones. The respondent indicated that a public statement was issued on this matter in 2002/2003 but no further details were provided.

A media report from May 19, 2002 indicates that while it was holding the presidency of the European Union, the government of Spain tabled a proposal for adopting harmonized regulations across the EU for identifying users of prepaid mobile phones. According to the report,

the Spanish proposal included the following statement:

The ministers recognises [sic] with concern that use of prepaid telephone cards under present conditions of anonymity for users prevents the implementation of the requirements and principles laid down in [the 1995 Council Resolution on the lawful interception of telecommunications]. ... The lack of regulation of anonymous prepaid telephone cards clashes with the need for law enforcement agencies to have access to telecommunications.⁵¹

The proposal also purported to claim that criminal use of prepaid mobile phones is “so hampering investigations into organized crime’ that the scope for action should at least be explored.” Such a statement implies the existence of evidence to support such a claim but the respondent to our study not able to provide information on any background studies in relation to proposed identity requirement for prepaid service in Spain or in the EU.

Related to Spain’s proposal, a European Commission bulletin from May 2003 reported its conclusions “on the tracing of the use of prepaid mobile telephone cards, in order to facilitate criminal investigations.” These conclusions were adopted on 8 May 2003 with the following wording:

Reiterating that the implementation of communications interception measures must respect the right to privacy laid down in Member States’ national laws and in Directive 2002/58/EC, the Council points out that prepaid telephone cards, used anonymously, constitute an attractive means of communication for individuals and organisations pursuing illegal ends. Considering

such use to be contrary to the principles of its resolution on the lawful interception of telecommunications, the Council recommends that Member States consider a set of appropriate requirements for tracing the use of prepaid card technology in connection with organised crime, paying particular attention to current technological progress in the field.⁵²

It may be reasonable to assume that the Council’s conclusions in 2003 are related at least in part to the Spanish proposal tabled in 2002. It is important to note that the conclusions do not specifically mention an identity requirement but instead provide a flexible framework that emphasizes technological means for tracing “the use” of prepaid cards rather than “the users” of the cards. The distinction may be important insofar as it recognizes that purchaser of a prepaid mobile phone might not be the same person that uses it.


The respondent was not able to indicate if Spanish mobile phone operators publish a code of practice for collecting customer information from prepaid account holders.

Spain does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement.

51 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>

52 European Commission. (2003, May 8). Bulletin EU 5-2003, Area of freedom, security and justice (10/18), 1.4.10. Council conclusions on the tracing of the use of prepaid mobile telephone cards, in order to facilitate criminal investigations. *Bulletin of the European Union*. Retrieved Dec. 20, 2004. Available <http://europa.eu.int/abc/doc/off/bull/en/200305/p104010.htm>

Sweden (SE)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
3,536 (49.4%)	4,333 (54.5%) ↑	5,003 (56.8%) ↑

Source: OECD (2005) *Communication Outlook*


The government of Sweden does not require mobile phone operators to collect customer information when activating prepaid service accounts. The government has neither issued a public statement nor sought expert or public opinion on this matter.

The respondent was not able to provide information on any background studies that might support or oppose an identity requirement for prepaid service in Sweden.

The respondent was not able to indicate if Swedish mobile phone operators publish a code of practice for collecting customer information from prepaid account holders.

Sweden does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement; however, the respondent indicated that emergency services in Sweden might have a resource similar to an IPND through the SOS Alarm initiative.

Switzerland (CH)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
2,154 (40.8%)	2,315 (40.4%) ↓	2,601 (42.0%) ↑

Source: OECD (2005) *Communication Outlook*

The Swiss government introduced mandatory identification for prepaid mobile phones in 2004. Article 15 of *la loi fédérale sur la surveillance de la correspondance par poste et télécommunication* (LSCPT) provides a general obligation for telecommunications providers on data retention.

Related to this statutory provision was an amendment made in June 2004 to regulations governing the collection of customer information under *l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication* (OSCPT). Article 19a of the OSCPT states:

Les fournisseurs de services de télécommunication doivent s'assurer que, lors de la vente de cartes SIM à prépaiement, les données personnelles du client (nom, prénom, adresse, date de naissance) sont enregistrées sur présentation d'un passeport ou d'une carte d'identité valable ou d'un autre document de voyage reconnu pour entrer en Suisse. Le type et le numéro de la pièce d'identité doivent également être saisis.⁵³

Mobile operators and customers in Switzerland were notified on June 2004 that the Swiss government would enact the prepaid policy on August 1, 2004, and that all prepaid SIM cards purchased after November 1, 2002 would have to be registered. The government set October 31, 2004 as the retroactive registration deadline, stating that customers not complying with the regulation would have their service cut-off by the mobile operator until registration was undertaken. Samples of Swisscom's customer notification website and its customer registration form are provided in Annex F and Annex G.

Shortly after the deadline passed, the European Digital Rights group published a news report stating that mobile operator Swisscom had been forced to disconnect 130,000 unregistered users of prepaid mobile phones as of November 30, 2004 for failing to comply with the regulation.⁵⁴

53 Le Conseil fédéral suisse. (2004, Jun. 23). Ordonnance sur la surveillance de la correspondance par poste et télécommunication. Retrieved Oct., 2005. Available http://www.uvek.admin.ch/imperia/md/content/g_s_uvek2/d/kommunikation/fernmelde/14.pdf

54 130,000 prepaid GSMs disconnected in Switzerland. (2004, Dec. 15). European Digital Rights: *EDRI-gram*. Retrieved Dec. 21, 2004. Available <http://www.edri.org/edrigram/number2.24/prepaid>

The introduction of prepaid regulations in Switzerland follows a widely disseminated media story reporting a successful anti-terrorist operation “Mont Blanc” that traced suspicious calls to Swisscom prepaid phones. It is believed that Swisscom was used partly because it offered an international prepaid roaming capability. Some time after this incident was reported, a commercial website selling prepaid cards announced “Swisscom International Prepaid SIM Card stopped working as of December 1st, 2003,” suggesting that the operator has discontinued this feature. This has not been verified. It is also interesting to note the comments of one counter-terrorism official in Europe who claimed that the mobile phone was “one of the most effective tools we had to locate Al Qaeda ... The perception of anonymity may have lulled them into a false sense of security.”⁵⁵

Under the new regulation mobile operators are now obliged to collect and retain for two years, the name, address, birth date, and record the number of an approved identification document (passport, etc.) prior to activating any prepaid account. This two year period applies from the date when prepaid service is terminated. The termination of a prepaid account corresponds to the conclusion of the contract between the customer and the provider, corresponding to the initial registration. An interpretation of the regulation by the government’s Department of Environment, Transport, Energy and Communication (DETEC) indicates that identity documents carried by certain groups within Switzerland, such as asylum seekers, are not valid for prepaid registration.⁵⁶

55 van Natta, Don and Butler, Desmond. (2004, Mar. 4). How Tiny Swiss Cellphone Chips Helped Track Global Terror Web. *New York Times*

56 Suisse Département fédéral de l’environnement, des transports, de l’énergie et de la communication (DETEC). (2005, Mar. 5). FAQ: enregistrement (a posteriori) des cartes SIM à prépaiement. Retrieved Oct., 2005. Available <http://www.uvek.admin.ch/>

While there is no legal obligation for customers to notify the mobile operator or government of any transfer of ownership or resale of a prepaid phone or SIM card, the original registered owner of the device could be liable for its subsequent use in illegal activities. The DETEC interpretation on this matter reads as follows:

Quelles peuvent être, pour la personne enregistrée, les conséquences de la revente ou de la transmission à un tiers de sa carte SIM à prépaiement ?

La revente ou la transmission d’une carte à prépaiement à un tiers n’est en soi pas punissable.

En revanche, la revente ou la transmission d’une carte à un tiers peut, en cas d’utilisation pour des actes punissables, avoir des conséquences pénales pour la personne enregistrée. Celle-ci peut, par exemple, être poursuivie pénalement pour entrave à l’action pénale ou lorsque les conditions du Code pénal en matière de participation ou de complicité sont remplies.⁵⁷

In cases where a mobile phone was purchased as a gift prior to the registration requirement coming into the force, only the active owner of it was required to register before the October 2004 deadline.

It is not known if opinion was sought on alternative measures to the registration requirement, but the government did form a committee following the terrorist attacks of 11 September 2001 in order to consider the issue as part of a wider package of anti-terrorism legislation. According to parliamentary records, the committee recommended against the proposal for a prepaid registration policy but this was rejected by the Council of States, which voted in favour of adopting the regulation. During debate on the matter, the argument was

57 *ibid.*

put forward that the measure would be of little consequence for most consumers but would act as a deterrent to criminal and terrorist acts. The following is the transcript of comments on this point made by government member Doris Leuthard speaking in the Swiss Parliament in March 2003 (in German):

Ich mache mir nicht die Illusion, zu glauben, mit der Registrierung werde inskünftig der organisierten Kriminalität das Handwerk gelegt, aber das Leben wird ihr schwerer gemacht. Es gibt Umgehungsmöglichkeiten, aber sie sind aufwendig. Man muss daran denken, und man kennt die Umgehungsmöglichkeiten. Es gibt solche Umgehungsmöglichkeiten im Übrigen auch beim Fälschen von Pässen, von Urkunden, von Autonummern. Das ist so, dass immer Missbrauchsmöglichkeiten entstehen.

Es besteht mit der Registrierung auch keine Gefahr, dass wir einen Polizeistaat eröffnen. Es geht am Schluss um das Abwägen zwischen den Gütern Sicherheit und Bekämpfung der organisierten Kriminalität auf der einen Seite und dem Persönlichkeitsschutz, dem Schutz der Privatsphäre, auf der anderen Seite.⁵⁸

It is not known if the government issues a regular report on law enforcement activities that includes information on prepaid users. However, in the


58 Conseil national Suisse. (2003, Mar. 12). Conventions des Nations Unies pour la répression du financement du terrorisme et des attentats terroristes à l'explosif. Ratification. Amtliches Bulletin. Retrieved Oct., 2005. Available http://www.parlament.ch/ab/frameset/d/n/4617/77205/d_n_4617_77205_77220.htm The following is a rough translation into English: "I do not put myself under the illusion to believe with the registration that organized criminality will be handicapped in the future but their world is made more difficult [by it]. There are evasion possibilities but they are complex. ... There are many evasion possibilities in falsifying passports, documents, license numbers [etc.]. There are always possibilities for abuse to develop. There is with the registration no danger that we will create a police state. The protection of the private sphere, on the one hand, must be considered against threats to national security and the fight against organized criminality on the other hand ..."

course of the parliamentary debate, statistics provided by Swiss law enforcement agencies that were cited by Leuthard, indicated some 60-70 per cent of intercept operations involved prepaid phones and that prepaid was used in 90-100 per cent cases of organized crime.⁵⁹

Mobile operators in Switzerland administer registration requirements and must disclose details on request from authorized government agencies. Operators are obliged by law to retain customer records for two years. It is not known if the government will produce a report on compliance with the requirement, or if it has acted to enforce compliance.

Switzerland does not maintain an integrated public number database (IPND) for the purpose of public safety or law enforcement. It is not known if the government has considered the introduction of an IPND either in the proceedings leading up to or following the introduction of prepaid regulations. Nevertheless, there is a special "Call Centre Information System" (CCIS) available for penal law enforcement authorities. The CCIS contains information about all phone numbers used in Switzerland, even if these numbers aren't included in publicly available number directories.

Turkey (TR)


 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
11,500 (62.4%)	17,125 (73.4%) ↑	20,851 (74.8%) ↑

Source: OECD (2005) *Communication Outlook*

Information was not received for Turkey.

59 *ibid.*

United Kingdom (UK)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
31,037 (69.1%)	33,758 (67.6%) ↓	36,000 (67.9%) ↑

Source: OECD (2005) *Communication Outlook*

The government of the United Kingdom does not require mobile phone operators to collect customer information when activating prepaid service accounts. The government has neither issued a public statement nor sought expert or public opinion on this matter.

The Interception of Communications Commissioner in the UK submits an annual report to the government, containing information on telecom interception activities. The report is required by the Regulation of Investigatory Powers Act 2000, is laid before Parliament and subsequently published; however, the document apparently includes a confidential annex detailing the operational successes achieved as a result of interception warrants that the Commissioner's office has reviewed. Although the Commissioner's report is not specifically about prepaid services, it might contain information about intercepts warrants issued in respect of prepaid mobile phones.

The respondent was not able to provide information on any specific background studies that might support or oppose identity requirement for prepaid service in the United Kingdom. The respondent did, however, provide a copy of a memo developed by the Mobile Broadband Group (MBG) in anticipation of calls for compulsory registration in the UK. The MBG is an association of the five major UK mobile network operators, all opposed to a mandatory registration policy for prepaid. The memo does not reflect the findings of any systematic study of the question, but instead introduces six points on which its opposition to prepaid registration is founded:

1. *Social inclusion*: the MBG argues that a prepaid registration policy would be “a retrogressive step” in the otherwise

successful role prepaid services have played in providing access to telephone service for socially disadvantaged groups such as “the homeless, the transient and those with poor credit records ...” The MBG suggests that a registration policy would eliminate or cut-off many of these customers from access to affordable telephone service.

2. *Practicality*: with over 35-million prepaid customers in the UK, the MBG argues that a registration policy faces practical barriers because retail outlets are not equipped to deal with the “logistics” of validating customer identification, and that it would require “a massive exercise to compel the existing base [of users] to comply with a registration scheme.” Moreover, the MBG claims that operators would be required to cut off service in cases of non-compliance, “causing major disruption to service and potentially putting customers at risk.”
3. *Effectiveness*: an additional burden on operators, according to the MBG, would be ensuring that the customer database is accurate and up to date. The MBG highlights the problem of compelling customers to notify operators of change of address or ownership of the mobile phone, suggesting that the government would have to introduce a coercive enforcement regime using fines or other penalties to force customers to comply with the requirement. Furthermore, the MBG claims that such efforts would be wasted because “it is ... hard to imagine that criminals, if they really wanted to cover their tracks, would not find a way of getting round the verification process, either by using a false identity or using a stolen phone.”
4. *Customer choice*: the MBG claims that prepaid customers choose the service partly because of the convenience of there being no associated paperwork. With respect to privacy concerns, the MBG suggests that customers “also believe that it is likely within their rights to buy and use telephony services without being answerable to the mobile operator or the government.”
5. *Cost*: in the absence of detailed cost/benefit analysis, the MBG used the UK's

DVLA (Driver and Vehicle Licensing Agency) database as a benchmark to estimate the impact of a prepaid registration policy. The DVLA database contains about 30-million vehicle registrations, with 3-million new vehicles added and some 4-million transfers of ownership each year. According to the MBG the cost of the DVLA is £170-million per annum to administer, which is offset by returns of £4-billion in vehicle excise duties and fines.⁶⁰ The MBG then draws a comparison with the cost of administering a national database for prepaid customers: Putative equivalent databases for [prepaid customers] would support a similar size (40 million) but, in all likelihood, would have to cope with a far larger number of transactions—particularly new registrations and customers churning between networks, which can amount to 20% of the whole base in any one year. Pre-pay SIMS are virtually disposable consumer goods, not significant personal assets. Furthermore the SIMS databases would not deliver anything like the law enforcement or financial payback of the DVLA, which is a profit centre for the Government. They may simply make it easier to trace the perpetrators of crime and malicious calls. It is easy to imagine that a database could cost at least £6 per SIM per annum to administer. £200-million on crime detection that could be better spent elsewhere.⁶¹

6. *Registrable services*: in spite of its opposition to a general registration policy for prepaid services, the MBG does recognize that such a measure is appropriate in certain specific cases:

The mobile operators are clear that it would be completely disproportionate to require a comprehensive verified database for all pre-paid subscribers. However, there may be examples where

it is appropriate that customer give their names and addresses (and have them verified by the networks) before they get access to specific services. One example of this today—and there may be others in the future—is the provision of passive location based services that are used [by parents] to locate children. ...

... Parents and carers gain comfort from these services but also want to be sure that location products are not used by people that have no bona fide interest in the whereabouts of their children. It is therefore quite right that mobile operators verify the identity of users of location both as a deterrent to miscreants signing up and as a record to fall back on in the event of misuse.

The United Kingdom does not have an Integrated Public Number Database (IPND) for the express purpose of public safety or law enforcement. However, UK authorities do make use of two independent databases for tracking stolen handsets—the Central Equipment Identity Register (CEIR) and the Mobile Equipment National Database (MEND)—but these do are not properly classified as IPND systems.⁶²

⁶² CEIR is an international service operated by the GSM Association that contains equipment identity details only: “The CEIR is a unique computer located in the GSM Association headquarters in Dublin, Ireland. It is a global central database containing information on serial number (IMEI) ranges of millions of handsets that have been approved for use on GSM networks. These approved handsets make up what is called the White List. There is also a CEIR Black List, which contains millions of handsets that should be denied service on a GSM network because they have been reported as lost, stolen or otherwise unsuitable for use.” [http://www.gsmworld.com/using/security/index.shtml]. MEND is a UK-based multipurpose service for tracking stolen property: “MEND is the UK’s largest database of property ownership and currently holds the records of millions of personal possessions and business assets and over 4.5 million items reported as lost and stolen.” [https://www.menduk.org/]

⁶⁰ Approximately \$352-million (CAD); (\$297-million USD); (€252-million EUR).

⁶¹ About \$12.50 (CAD) per SIM, per annum.

United States (US)

 Market size (000s) and share for prepaid mobile phones		
2001	2002	2003
11,565 (6.0%)	11,565 (8.2%) ↑	11,565 (7.3%) ↓

Source: OECD (2005) *Communication Outlook*

The government of the United States does not require mobile phone operators to collect customer information when activating prepaid service accounts. However, there does appear to have been an effort to introduce regulations for prepaid communication services:

In early 2003, a Pennsylvania state legislator introduced legislation that would have required stores to record the identity of everyone buying a phone card. The [International Prepaid Communication Association] was instrumental in killing that bill, but it may be symptomatic of the kind of legislation we may see in the future.⁶³

Perhaps of greater concern to the prepaid telecom industry in the United States is possible scrutiny following from provisions in the Intelligence Act of 2004 to increase powers of authorities to obtain records from businesses “whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters.” It has been reported in the United States that prepaid phone cards were associated with terrorist activities, including the Oklahoma City bombings.⁶⁴

In June 2004, the International Prepaid Communication Association (IPCA) announced that it would form a committee to look into call detail records (CDR) storage and develop a consensus position on anti-terrorism legislation that might affect the prepaid industry. IPCA has been encouraged by the FBI and DEA in the

United States “to promote industry standards for CDR storage” and to provide expert advice on “call hopping,” which is described as

... a method of using one phonecard to call another phonecard switch, and use the second phonecard to call a third switch and then make the call to the desired destination. The multiple CDRs generated are difficult to trace and particularly difficult to trace expeditiously. ... [and] it is impossible to tell whether a phonecard switch is carrying a call from another phonecard’s switch.⁶⁵

One aim of the IPCA committee work was purported to be the creation of a centralized database of prepaid CDRs to support law enforcement activities in the United States, possibly as an alternative to a customer registration policy. An informal conversation with Regulatory Affairs department of the Cellular Telecommunications Industry Association (CTIA) indicated that law enforcement agencies in the United States routinely employ a range of methods, including so-called “trap and trace” to identify telephone users.

The prepaid industry has also noted problems with regulatory compliance more generally:

It is common knowledge in the prepaid phonecard industry that few laws applying to prepaid phonecard issuers are strictly enforced. ... [W]hen a new phonecard law is passed, the common scenario is that the more legitimate companies will comply and bear the costs of the new rules. But, less legitimate companies will not comply and the result will be that they will have a competitive edge over the companies in conformance.⁶⁶

63 Harding, Richard A. (2004, May). “Terrorism’s impact.” *Intele-Card News*. Retrieved Sept. 29, 2004. Available http://www.intelecard.com/ipcaview/03ipcaview.asp?A_ID=381

64 *ibid.*

65 Segermark, Howard. (2004, Oct. 18). “Prepaid call detail records: an anti-terrorism tool.” *The Prepaid Press*. Retrieved Oct, 2005. Available http://www.prepaid-press.com/news_detail.php?t=paper&id=598

66 *ibid.*

It is not known, however, if any formal background studies have been undertaken in the United States specifically with respect to a registration policy for prepaid services. Similarly, no information has been obtained to provide an update on the IPCA committee's work (or subsequent industry-led initiatives) to examine the use of call detail records to support law enforcement and national security activities in the United States.

The United States does not have a national Integrated Public Number Database for the express purpose of law enforcement or public safety.

The following sections present a summary of observations and findings from the survey.

Justification for and against prepaid registration

The justification in support of a prepaid registration requirement in most countries has been expressed in terms of improving efficiency for law enforcement and national security. One exception was Ireland, where the call for registration was concerned with the protection of minors from adult content on 3G networks. Other reasons given to support prepaid registration included support of emergency services, maintenance of commercial directory services and enabling local number portability, as well as for certain value-added services (e.g., location based services).

The justification against prepaid registration requirement has been expressed in terms of cost to business, privacy concerns in terms of unintended use and disclosure of customer records, and questions about the effectiveness of such a measure to deter or otherwise reduce criminal activity associated with prepaid phones.

Feasibility of implementing and enforcing regulatory measures

In most cases where prepaid registration has been introduced there has been little information forthcoming about how authorities intend to monitor and enforce compliance, aside from disconnecting unregistered customers. Two exceptions are in Australia and Norway where concerns about point of sale identity verification and validation has received considerable attention. In Australia the matter remains unresolved pending the outcome of a public consultation to consider alternative methods.

In some countries, customers are required to report to the mobile operators each transfer

of ownership or second-hand sale of a prepaid mobile phone. This may be especially problematic in countries where large numbers of mobile phones are bought and sold through informal distribution channels.

There is still some ambiguity as to how long mobile operators are required to retain information collected from prepaid customers and how to determine when a customer “terminates” their prepaid service. As well, there is some uncertainty as to the division of responsibility between mobile operators and customers with respect to upkeep of prepaid registration records and any related liability issues.

There was very little information from government authorities concerning the anticipated cost of the registration requirement to mobile operators or customers, or about the cost to government for monitoring and enforcing compliance. The UK Mobile Broadband Group estimates that the cost of a registration scheme would be £6 (\$12.50 CAD) per customer per annum.

Possible use of alternative measures

There was no indication to suggest that alternative measures for identifying prepaid users have been tested or adopted in any of the countries that responded to the survey. One notable exception to this is in Australia, where the regulator has proposed an electronic verification of customers during “post-sale” activation process rather than at the point of sale.

In the case of Germany and the Netherlands, there is some indication that IMSI-catcher technology has been used by law enforcement to identify mobile phone users. Further details are available but have not been translated into English (see country profile for Germany).

In the United States the prepaid communications lobby has suggested the standardization and centralization of prepaid Call Detail Recording

(CDR) systems possibly to draw attention away from calls for a prepaid registration requirement.

Impact on IPND

Statements made by the Australian regulator in its July 2005 discussion paper, indicate that failure to validate and verify prepaid mobile phones will have a significant impact on the accuracy and usefulness of an Integrated Public Number Database.

A number of countries, such as Germany and the Netherlands, require that operators make their customer records available to law enforcement agencies, but none have reported having a standalone national IPND. Experience from Australia indicates that even with a registration requirement, customer records for mobile services and prepaid mobile services tend to have lower accuracy than records for landline customers.

Experience from Australia also suggests that a robust and efficient identity validation and verification system must be in place in order to ensure accurate record keeping and for the maintenance of an IPND system.

~ ~ ~

The purpose of this report has been to present information gathered about the regulation of prepaid mobile phone services across a range of countries comparable to Canada. Readers are reminded that the purpose of this report has not been an in-depth analysis of the findings but rather to provide a body of data with which to support public deliberation on the question of privacy rights and prepaid communications services in Canada and elsewhere.

It is hoped that the information presented in this report will assist other researchers and policymakers to undertake in-depth analysis and investigation into specific details when and where it is seen to be fit to do so.

Annex A: Survey Instrument

PART A: All respondents are asked to complete this section

The regulation of prepaid mobile phone service or SIM cards in your country.

A1 Does the government of your country require the identification of users of prepaid mobile phones or mobile phone SIM cards?

A2 Can you provide source information for any government documents or public policy statements in connection with the introduction of these requirements?

If so, please indicate the approximate date and source of this statement or statements:

A3 Has your government sought or otherwise received expert or public opinion concerning the introduction of identity requirements for prepaid mobile phone service, whether or not these requirements are now in force?

If so, please indicate the approximate date of this consultation and the source of any public documents about it.

A4 Has your government sought opinion on alternative means for identifying mobile phone customers that do not depend on the collection of subscriber information at the point of sale?

If so, please indicate the approximate date of this consultation and the source of any public documents about it.

A5 Does your government produce or make available a report on law enforcement or national security activities that might include information about prepaid mobile phone users?

If so, please indicate as much source information (date, title, etc) as possible about this report.

PART B: Please answer this section if your country has an identity requirement or will soon introduce an identity requirement for prepaid mobile phone service.

B1 Can you provide information about any background studies produced by any organization (public or private) within your country that explicitly support an identity requirement for prepaid mobile phone service?

If so, please indicate as much source information (date, organization, title, etc) as possible about these studies.

B2 What organization(s) is/are designated to administer the identity requirements for prepaid mobile phones in your country?

B3 Does this organization produce a regular report on compliance with these regulations?

B4 Is this report available to the public?

If so, please indicate as much source information (date, title, etc) as possible about this report.

B5 Has this organization ever taken action to enforce compliance?

Please indicate any specific details of this action

PART C: All respondents are requested to answer the questions in this section.

C1 Can you provide information about any background studies produced by any organization (public or private) within your country that have explicitly opposed an identity requirement for prepaid mobile phone service?

If so, please indicate as much source information (date, organization, title, etc) as possible about these studies.

C2 Do any mobile phone operators in your country publish a corporate policy regarding the collection of customer information from prepaid mobile phone subscribers?

If so, please indicate as much source information as possible about these corporate policies.

C3 Have the mobile phone operators or retailers in your country published an industry-wide code of practice regarding the collection of customer information from prepaid mobile phone subscribers?

If so, please indicate as much source information as possible about this code of practice (e.g., organization, website, press releases, etc.)

PART D: *All respondents are requested to answer the questions in this section.*

D1 Does your country maintain an 'integrated public number database' containing the details of all telephone subscriber information for the purpose of public safety or law enforcement?

If so, please indicate as much source information as possible about the organization designated to operate this database, as well as the year it was introduced into service.

D2 Does the database administrator issue a regular report concerning the use of the database in your country?

If so, please indicate as much source information (date, title, etc.) as possible about this report.

D3 Does the database administrator apply any form of measurement concerning the usefulness of the integrated public number database for law enforcement or public safety purposes?

If so, please describe these measurements.

D4 Does the database administrator or any other organization apply any form of cost/benefit measure concerning the database in your country?

If so, please indicate as much as possible about this measure.

PART E: *All respondents are requested to respond to the questions in this section.*

E1 Do you have any additional comments or further information you wish to add to this survey?

E2 Please fill in your contact information below to validate the survey. We will keep these details confidential at your request (see question E3).

E3 Do you want us to keep your name and other contact information confidential when we publish the results of this survey?

E4 May we contact you if we have additional follow-up questions from this survey?

E5 Do you wish to receive the results of the report when they become available?

End of survey

Annex B: Summary of Responses to the Survey

The following table provides a raw summary of survey responses. Readers should note that the information contained in the country profiles section of the report differ slightly from details contained in this table. This is due in some cases to differences in the interpretation of the questions. In other cases, additional follow up research led the research team to findings that affected the interpretation of the initial responses.

Country	code	Part A	Part B	Part C	Part D	Part E
Australia	AU	Yes identification requirement in 1997 Telecoms Act; it applies to all fixed and mobile services; not known if gov't sought opinion when introducing requirements but press release issued at time of introduction of requirement; no opinion sought on alternative means; yes government reports on lawful access activities (see Part D);	Yes background studies might be found in public debates leading to 1997 Telecoms Act; each carrier administers identity requirements; yes report(s) are issued on compliance[?]; uncertain if report is available to public but ACMA manages many compliance functions and issues annual report; yes action taken to enforce compliance (no details);	No studies opposed to identity requirement; yes most operators publish a corporate policy about identity collection according to privacy legislation (e.g., Telstra website); no industry-wide code of practice as presence of legislation negates any need for it;	Yes there has been an IPND since 1998, operated by Telstra on behalf of industry; it is subject to annual audit until 2006; fact sheet available on ACMA website; no report issued by Telstra but ACMA includes it in annual report; no measure of usefulness applied to IPND; no cost/benefit measure applied;	Response provided by industry executive;
Austria	AT	No identification requirement;	--	--	--	No formal response;
Belgium	BE	No identification requirement; no public statements; not known if opinion sought on introduction of such requirements; no opinion sought on alternative means; no report issued about lawful access activities;	Not applicable	No background studies that oppose identity requirements; no mobile operators publish corporate policy on identity collection from prepaid; no industry-wide code of practice published;	No IPND or related administrative activities;	Response provided by industry executive;
Canada	CA	No identification requirement	Not applicable	No background studies that oppose identity requirements but public statements made by Privacy Commissioner, civil society, and mobile carriers; no industry code of practice published;	No IPND or related administrative activities	Response provided by university researcher;

Country	code	Part A	Part B	Part C	Part D	Part E
Czech Republic	CZ	No identification requirement; yes opinion sought through discussions held in Parliament in May 2005; not known if opinion sought on alternative means; no report made available about lawful access activities;	Not applicable	Not known if any studies opposed to identity requirement; however , some discussion reported between Czech regulator and Mobile Network Operators Association with no reported outcome; yes mobile operators obliged to publish corporate policy on general terms and conditions of service, under which prepaid registration is voluntary; no industry-wide code of practice has been published;	No IPND for law enforcement but incumbent operator maintains a public directory that does include mobile phone numbers of subscribers who have requested their publication ;	Response provided by industry executive;
Denmark	DK	No identification requirement; no public statements; no opinion sought on introduction of identity requirements; no opinion sought on alternative means; no report issued on lawful access activities;	Not applicable	Not known if any studies opposed to identity requirement; not known if mobile operators publish corporate policy on identity requirements; not known if industry-wide code of practice has been published;	No IPND; however operators are obliged by law to operate their own customer number databases [not known if prepaid is included]; not known if report is issued about the use of these databases or their value to lawful access	Response provided by university researcher
Finland	FI	No response	--	--	--	--
France	FR	Yes identification requirement to fulfil statutory requirements for lawful access and formally requested by Ministry of Interior in 1997; not known if opinions sought when introducing requirements; no opinion sought on alternative means; not known if report issued on lawful access activities;	No studies that explicitly support identity requirement; each operator administers own identity requirements; no report issued on compliance; no action taken to enforce compliance;	No information provided about background studies that oppose identity requirements; not known if mobile operators publish corporate policy on identity collection [?]; no industry-wide code of practice has been published;	No IPND or related administrative activities;	Response provided by industry executive;

Country	code	Part A	Part B	Part C	Part D	Part E
Germany	DE	Yes identification requirement established in Telecoms Act, sec. 111 dated 22 June 2004; not known if opinions sought when introducing requirements; not known if opinion sought on alternative means; however , IMSI-catcher has been used and is allowed by legislation; no report made available on lawful access activities;	No studies that explicitly support identity requirement; however , some related research on telecom surveillance has been published; regulator (BNetzA) is responsible for securing compliance; no report issued on compliance; however , reports might appear in future given that requirements introduced recently in 2004; not known if action taken to enforce compliance;	Yes information provided about background studies that oppose identity requirements [?]; however , a complaint was recently issued to German Federal Constitution Court (20 June 2005) challenging the new Telecoms Act, including identity requirement for prepaid; not known if mobile operators publish corporate policy on identity collection; not known if industry-wide code of practice has been published;	No IPND or related administrative activities;	Response provided by university researcher;
Greece	GR	No identification requirement; yes policy statement from the government protect anonymous prepaid usage; no opinion sought on alternative means, however, the Hellenic Data Protection Authority drew attention to the issue; no report on lawful access activities.	Not applicable.	Yes information provided about background studies that oppose identity requirements (Law 2774/1999); no mobile operators publish corporate policy on identity collection; no industry wide code of practice exists.	No IPND or related administrative activities;	Response provided by government official;
Hungary	HU	Yes identification requirement; yes policy statement from government under Act No. C of 2003 on Electric Communication; not known if opinion sought on alternative means; not known if report issued on lawful access activities.	Not known if studies done to support identity requirement; not known if reports on compliance; not known if compliance enforced.	Not known if studies opposed identity requirements; yes mobile operators publish corporate policy on identity collection; no industry wide code of practice needed, as appropriate legislation exists.	No IPND or related administrative activities;	Response provided by government official;
Iceland	IS	No response	--	--	--	--

Country	code	Part A	Part B	Part C	Part D	Part E
Ireland	IE	No identification requirement; however, the government sought to build a national register of 3G phones in 2003-04; not known if opinions sought on introduction of identity requirements; no opinion sought on alternative means; no report issued on lawful access activities;	Not applicable	Not known if any studies opposed to identity requirements; however, mobile industry lobbied against proposed prepaid registration [?]; yes operators publish corporate policy on identity collection in accordance with privacy legislation; moreover , voluntary registration for prepaid is encouraged by operators, some of whom offer call credit [B2]; yes industry-wide code of practice published in 2004 to promote safe and responsible use of prepaid mobile phones, and to allow parents to access children's prepaid records and account details;	No IPND or related administrative activities;	Response provided by industry executive;
Italy	IT	Yes (unconfirmed report);	--	--	--	--
Japan	JP	Yes identification requirement established in Law #31 - on confirmation of personal identification of the subscribers, effective April 2005; yes opinion sought through hearings with operators and consumer representatives; no opinion sought on alternative means; no report issued on lawful access activities.	No studies done that support identity requirement; regulator (MIC) and police (NPA) administer the identity requirements; no reports on compliance; yes action taken to enforce compliance in form of criminal charges, as well as PR campaigns.	No background studies that oppose identity requirements; no corporate policy published, but operators announce activities that comply with law; no industry-wide code of practice.	No IPND or related administrative activities	Response provided by industry executive;
Korea	KR	No response	--	--	--	--
Luxembourg	LE	No response	--	--	--	--

Country	code	Part A	Part B	Part C	Part D	Part E
Mexico	MX	No identification requirement; not known if expert opinion sought the introduction of requirements; not known if opinion sought on alternative means; no report issued on lawful access activities.	Not applicable;	No background studies opposing identity requirements; no mobile operators publish corporate policy; no industry wide corporate policy established	No IPND or related administrative activities;	Response provided by civil society organization;
Netherlands	NL	No identification requirement; yes expert opinion sought when considering requirements; yes alternative means of identifying phone numbers was demonstrated without registration; no report issued on lawful access activities	Not applicable;	Not known if background studies were published that oppose identity requirements; yes mobile operators publish corporate privacy policy, service incentives for supplying identification information are provided, details used for direct marketing; no industry-wide code of practice exists.	No IPND, however , mobile operators submit subscriber information to a database that operates like an IPND and can only be accessed by law enforcement agencies through a third party under authority of the Ministry of Justice; yes the third party issues a report concerning use of database; don't know if the value of the database is assessed.	Response provided by industry executive;
New Zealand	NZ	No identification requirement; no opinion sought on possibility of requirements; no opinion sought on alternative means, however , the identification of mobile phone activity in prisons is being investigated; no report on lawful access activities.	Not applicable;	No background studies opposing identity requirements published; no operators publish corporate policy on identity collection; no industry-wide code of practice.	No IPND or related administrative activities.	Response provided by industry executive;
Norway	NO	Yes identification requirement established in Electronic Communications Act and related committee reports between 2001-2003; yes opinion sought through public hearing process; no opinion sought on alternative means; yes report issued on lawful access activities;	Not known if studies done that support identity requirement; regulator (NPT) administers the identity requirements; yes reports on compliance; yes report available to public (included in regulator's annual reports); yes action taken to enforce compliance in the form of letters sent to operators by regulator;	No information provided about background studies that oppose identity requirements; not known if operators publish corporate policy on identity collection; however , Telenor has information about registration procedures on website; no industry-wide code of practice published;	No IPND or related administrative activities;	Response provided by university researcher;

Country	code	Part A	Part B	Part C	Part D	Part E
Poland	PL	No identification requirement; no statement issued, however , the registration of prepaid phones to prevent terrorism and crime was proposed by the Ministry of Internal Affairs and Administration, Internal Security Agency and Ministry of National Defense; No opinion sought on registration; not known if opinion sought on alternatives; not known if report issued on lawful access activities.	Not applicable;	Not known if background studies produced opposing identity requirements, however , mobile phone operators opposed registration measures due to the financial costs they would incur; yes mobile phone operators publish corporate policy on identity collection; no industry wide code of practice.	No IPND or related administrative activities.	Response provided by government official;
Portugal	PT	No identification requirement; no statement issued; don't know if opinion sought when introducing requirements; don't know if opinion sought on alternative means; no report issued on lawful access activities.	Not applicable.	No background studies that oppose identity requirements; no mobile operators publish corporate policy on registration; no industry-wide code of practice.	No IPND or related administrative activities.	Response provided by industry executive;
Slovak Republic	SK	Yes identification requirement regulations explained in Act 610 of 2003; not known if opinions sought on implementing requirements; no opinion sought on alternative means of identification; not known if report on lawful access is published.	Not known if background studies support identity requirement; each operator collects and retains identification information; not known if reports on compliance published; yes compliance has been enforced by law enforcement requests, and is subject to fines by Telecommunications Office.	Not known if background studies published that oppose identity requirements; yes operators publish corporate privacy policy; no industry-wide code of practice is needed as appropriate legislation exists.	No IPND or related administrative activities.	Response provided by government official;

Country	code	Part A	Part B	Part C	Part D	Part E
South Africa (non-OECD)	--	Yes identification requirement established in Act 70 of 2002, but will only be implemented at the end of 2005, however , the proposed paper-based collection system may be supplanted by an electronic registration process, due to extensive use of informal distribution channels; yes public opinion sought during legislative process; no opinion sought on alternative means; no report on lawful access activities.	No background studies supporting identity requirement published; each operator collects and retains identification information; no reports on compliance; no action taken to enforce compliance, however , severe penalties are enabled in the act for non-compliance.	No background studies published that oppose identity requirement; yes operators publish corporate privacy policy; no industry-wide code of practice.	No IPND or related administrative activities.	Response provided by industry executive;
Spain	ES	No identification requirement; yes statement issued in 2002/2003 by a previous government on desire to mandate identification of prepaid customers; not known if opinions sought on possibility of requirements; no opinions sought on alternative means; no report on lawful access activities.	Not applicable;	No background studies opposing identity requirements published; not known if operators public corporate policy on identity requirements; no industry-wide code of practice.	No IPND or related administrative activities.	Response provided by industry executive;
Sweden	SE	No identification requirement; no statement issued; an enquiry into introducing requirements has not resulted in regulations; not known if opinion sought on alternative means; every year the government issues a report to the Parliament on privacy and telecommunications; no report issued on lawful access activities;	Not applicable	Not known if background studies opposing identity requirements published; yes mobile operators publish corporate policy on identity collection; however , details may be vague; no industry-wide code of practice for identity collection;	Yes there is a public safety database operated by public institutions (SOS Alarm); yes administrator publishes a report concerning use of the database; however , this may be confined to financial reporting; not known if any measures applied to assess the value of the database;	Response provided by university researcher;

Country	code	Part A	Part B	Part C	Part D	Part E
Switzerland	CH	Yes identification requirement announced in government press release of 23 June 2004; not known if opinion sought when introducing requirements (see Part C); no opinion sought on alternative means; no report made available on lawful access activities;	No information provided about background studies that support the identity requirement; each carrier administers identity requirements; no reports on compliance; reports are not available to public; no reported action taken to enforce compliance;	No information provided about background studies that oppose identity requirements; however , parliamentary record indicates a commission asked to study the question recommended against it; yes mobile operators publish corporate policy on identity collection; no industry-wide code of practice has been published	No IPND or related administrative activities;	Response provided by industry executive;
Turkey	TR	No response	--	--	--	--
United Kingdom	UK	No identification requirement; no opinion sought on introducing requirements; no opinion sought on alternative means; yes report issued by Interception Commissioner to Parliament (might include prepaid cases);	Not applicable	Not known if any studies that oppose identity requirement; yes some mobile operators encourage voluntary registration but have an internal policy that does not support compulsory registration; however , Orange is reported to have a corporate policy of compulsory registration of prepaid for commercial reasons; no industry-wide code of practice in identity collection; however , Mobile Broadband Group opposes compulsory registration;	No IPND; however , CEIR and MEND ("the Register") are databases maintained for tracing stolen equipment;	Response provided by industry executive
United States	US	No identification requirement; no opinion sought on the introduction of registration; no opinion sought on alternative means; not known if report issued on legal access activities.	Not applicable	No background studies opposing identity requirements; not known if mobile operators publish corporate policy; yes a voluntary industry-wide code of practice exists.	No IPND; however, a nation-wide public numbers directory for landlines is established.	Response provided by civil society organization;

Annex C: Vodafone Japan Customer Notification

Notice

14 April 2005

Vodafone K.K. to confirm identification of prepaid customers

Vodafone K.K. announces today that it will introduce an additional measure on 25 April 2005 to confirm the identification of all customers using prepaid handsets sold under the Vodafone Prepaid Service* to prevent the inappropriate use of prepaid handsets in Japan.

A change will be implemented to confirm the identity of all prepaid customers, including existing customers that purchased prepaid handsets in the past. Those unable to provide the requested information within a certain period will have their lines suspended.

Details of the measure are as follows:

- (1) Via its website, mail and other communication methods, Vodafone K.K. will request that prepaid customers register their ID information. The following types of customers are affected:
 - Customers who are currently using prepaid handsets, but did not register ID information
 - Customers who registered ID information but have since seen a change in registration detailsCustomers who register ID information with Vodafone K.K. will be treated as Vodafone K.K. subscribers. Customers who registered ID information at time of purchase, but have since transferred prepaid mobile handsets to third parties, and are not using them, are required to report this information to Vodafone K.K.
- (2) Customers will be able to register their ID information at Vodafone shops nationwide from 25 April until 31 October 2005.
- (3) From November 2005, Vodafone K.K. will begin suspending the lines of customers unable to provide ID information within the given timeframe above.

In addition to implementing this measure to confirm the ID of prepaid customers, Vodafone K.K. will introduce a transfer system for its prepaid service to manage customer information. Customers wishing to transfer a prepaid handset to third parties will be required to report this information to Vodafone K.K.

Vodafone K.K. has already implemented the following measures for prepaid service ID confirmation:

- (1) Since December 2004, at time of purchase, customers can only use prepaid handsets after their ID information has been confirmed and registered on Vodafone K.K.'s customer information system.
- (2) Since December 2004, Vodafone K.K. has been confirming the ID of existing prepaid customers when requested by municipal governments, and has suspended lines if customers failed to provide the information requested.

*Vodafone Prepaid Service and Pj. Pj is a prepaid service that offers handsets mainly in the Tokai region.

- Vodafone Prepaid Service and Pj are trademarks of Vodafone K.K.
- Vodafone is a registered trademark of Vodafone Group Plc.
- Vodafone Group is the world's leading mobile carrier and as of the end of December 2004, had equity interests in 26 countries and 416.4m venture customers, with a further fourteen partner networks.

About Vodafone K.K.

Vodafone K.K. is a leading mobile operator in Japan with over 15 million customers and a subsidiary of Vodafone Group Plc, the world's largest mobile community. The Tokyo-based company offers a wide range of sophisticated mobile voice and data services including Vodafone live!, which provides mail and internet access to 85% of its customers, and pioneered the picture messaging service called Sha-mail first introduced in November 2000. In December 2002, Vodafone K.K. launched the world's first commercial 3G W-CDMA service based on 3GPP international standards. Vodafone K.K.'s 3G service offers its customers rich content and roaming on 155 networks in 116 countries and regions as of 31 March 2005. For more information, please visit www.vodafone.jp

Annex D: Translation of NPT Letter of 29 September 2004

Providers of public mobile phone services
as per attached address list

Our ref: Our date:
04/00631-411.2 29.09.2004

Your ref: Your date:

Executive Officer:
Einar Meling
E-mail:
einar.meling@npt.no

Registration of end-users, particularly with regard to pay-as-you go customers

The (Norwegian) Post and Telecommunications Authority (PT) refers to previous correspondence in this matter and to the meeting which took place at the offices of PT on 25 August 2004 between representatives from the providers, the Norwegian National Authority for Investigation & Prosecution of Economic and Environmental Crime (*Økokrim*), The Norwegian National Police Directorate (*Politidirektoratet*), Oslo Police District and PT.

Paragraph 6-2 of the Electronic Communication Networks and Electronic Communication Services regulation (referred to as the "*Ekom* regulation"), states that providers of public telephone services are obliged to keep a register of every end-user's name, address and the number/address of the service. The register must contain information which enables the registered users to be unambiguously identified.

Based on information it has received, the Post and Telecommunications Authority considers it necessary both to clarify what this registration requirement involves, and to guarantee its harmonised implementation. Below is a clarification of the requirements set by PT for the implementation of the registration of pay-as-you go customers in accordance with paragraph 6-2 of the *Ekom* regulation.

1. Requirements for the information

The registration of end-users which the providers of public telephone services are obliged to carry out must contain information which makes unambiguous identification of the registered users possible. The stipulation refers to section 2 of paragraph 6-3 in the *Ekom* regulation, which gives examples of the type of information which makes unambiguous identification possible.

PT takes the view that the registration requirement is met as long as the registered information collectively makes it possible to identify the end-user in an unambiguous way. This means that there is no absolute demand for a personal identification number (*equiv. to National Insurance Number*). The end-user's name, date of birth and address will in nearly all cases be sufficient to identify a particular person. When registering customers who are foreign nationals, their nationality will have to be noted in addition to their name, address and date of birth.

If the providers nevertheless should have a just requirement for collecting an end-user's personal identification number in order to be able to provide unambiguous identification, this information must be

treated in accordance with the (Norwegian) Personal Data Act (*Personopplysningsloven*). In cases where obtaining a person's personal identification number is regarded as necessary, PT considers that the rationale laid down in the regulation is sufficiently accommodated because such information is available at the time of registration. In PT's view, subsequent retention of such information is not necessary to fulfil the requirement for registration according to paragraph 6-2 of the *Ekom* regulations.

Companies wishing to give their employees pay-as-you-go subscriptions will have to register such subscriptions to a responsible person and with the same requirements for personal information as with registration of private customers.

2. Quality assurance of information

The requirement that the information must make unambiguous identification possible means that the information registered at the time of registration needs to be of a certain quality.

So far, quality checks of information have been carried out by the providers by comparing the information they are given with information in the national population register (*Folkeregisteret*). However, the Authority for Investigation & Prosecution of Economic and Environmental Crime (*Økokrim*) and the police want stricter identity control based on the Money Laundering Act (*Hvitvaskingsloven*), which means that customers have to provide identification before a relationship with the provider can be established. The providers feel that this will be difficult to carry out in practice and too strict requirements will have negative consequences for the sale of pay-as-you-go cards.

Beyond the demand for unambiguous identification, the Act on Electronic Communication (*Ekomloven*) and the *Ekom*-regulation do not give any clear leads on the type of quality assurance required for information. Paragraph 5 of the Money Laundering Act, however, states clearly that identity checks must be done face to face. The above-mentioned laws thus have a very different basis, and for that reason PT doubts whether the Money Laundering Act can be used as a model for interpreting the law and regulations on electronic communication. PT thus finds it difficult to set an absolute demand that customers must provide ID when they buy pay-as-you-go cards. This also needs to be seen in the light of the many different places which sell top up cards.

A minimum requirement for quality assurance is, however, that the registered information is checked against information in the national population register (*Folkeregisteret*). Applications for on-line permission or other permission can be sent to the Central Office for Population Registration (*Sentralkontoret for Folkeregistrering*). As an equivalent check for customers who are foreign nationals would not be possible, PT will at a later stage give further consideration to the registration of these customers if there proves to be a large number of false registrations in this group.

3. Time of registration

One of the main considerations behind the requirement for registration is that it needs to be possible to trace the owner of a telephone subscription for (criminal) investigation purposes. It is therefore of critical importance that when taking out a new subscription, the customer should not be able to use the telephone until the registration is complete.

In order for the registration to comply with paragraph 6-2 in the Ekom-regulations, providers must thus make sure that necessary information is registered and quality assured before the SIMcard of the mobile phone can be activated. This could for example happen by on-line registration at the point of sale, or by making the very first telephone call to customer service.

4. Closing dates for the registration of end-users

The following closing dates for registration duty will apply:

- All new pay-as-you-go customers must be registered in accordance with the above by 1 January 2005. From the same date it will no longer be possible for unregistered pay-as-you-go customers to top up their cards.
- All end-users must be registered in accordance with the above by 1 June 2005. From that same date, unregistered user-numbers or numbers where the registration clearly is false, will be closed to traffic.

Any objections to these time limits must be sent to PT by 13 October 2004.

Yours faithfully

Willy Jensen Arne Litleré

cc.: Norwegian Ministry of Transport and Communications (*Samferdselsdepartementet*)
Espen Skjerven, Norwegian National Authority for Investigation &
Prosecution of Economic and Environmental Crime (*Økokrim*)
Leif A. Halvorsen, Oslo Police
Annicken Iversen, The National Police Directorate (*Politidirektoratet*)
Norwegian Data Inspectorate (*Datatilsynet*)

Annex E: Translation of NPT Letter of 8 November 2004

**Providers of public mobile phone services
as per attached address list**

Our ref:
04/00631-411.2 08.11.2004

Our date:

Your ref:

Your date:

Executive Officer:

Einar Meling

E-mail:

einar.meling@npt.no

Registration of end-users, particularly with regard to pay-as-you go customers

We (The Norwegian Post and Telecommunications Authority (PT)) refer to our letter dated 29 September 2004. In this letter, we outlined the requirements we wanted established in connection with information, quality assurance of information and time of registration, particularly with regard to **pay-as-you go customers**. PT further established time limits for the registration of end-users in accordance with the requirements, but giving providers the opportunity to raise objections to the time limits. The demand for registration covers all providers of public telephone services, but is mainly relevant for providers with pay-as-you-go customers in this context.

NetCom and Sense have raised objections to the requirements. The companies particularly point to the requirement that a mobile phone would not be enabled for use until the user has been unambiguously identified. The companies feel that in order to be able to meet this requirement a 24-hour customer service centre will have to be established, and this would be both expensive and time-consuming. The companies therefore propose that it should still be possible to use the telephone for a limited period before the user is unambiguously identified.

PT cannot agree to this request. We feel that such an arrangement would undermine the aim of paragraph 6-2 of the *Ekom* regulations. The reactions to our letter of 29 September 2004, however, appear to show that it was interpreted to mean that providers are locked into just one way of meeting this requirement. PT would therefore like to emphasise the following:

The main requirement is that public telephone services should not be enabled for use until the user/owner has been registered in an unambiguous way. It is the providers of such services who are responsible for fulfilling this requirement.

The requirement appears to be satisfactorily met as far as subscription customers are concerned, both for landlines and mobiles, but not for pay-as-you-go customers. For pay-as-you-go customers the requirement could be met e.g. by the customer providing identification at the point of sale. In such cases the customer would be able to use the mobile phone immediately after the seller has registered the customer's name and address in line with the identification provided. The provision of ID at the point of sale would also guarantee unambiguous identification of persons who are not registered in the National Population Register (*Folkeregisteret*). The providers can also use other methods with regard to establishing customers' identity, as long as the above-mentioned main requirements are met. However, as far as foreign nationals temporarily staying in Norway are concerned, it is difficult to envisage any other method than the provision of ID to guarantee unambiguous identification.

For the sake of good order, PT would like to remind providers that they also have a responsibility to ensure that the information they hold on existing customers is correct in relation to the demand for unambiguous identification. PT has legal authority to set further demands pursuant to the provisions of paragraph 10-6 of the *Ekom* Act if we learn of false registrations.

NetCom and Sense also request that PT postpone the deadlines for the introduction of the registration requirement. PT is able to postpone the deadlines as follows:

- All new end-users of public telephone services, including pay-as-you-go customers, must be registered in accordance with the requirements by 1 February 2005. From that same date, unregistered pay-as-you-go customers will no longer be able to top up their mobile cash cards.
- In accordance with the requirements, all end-users of public telephone services must be registered by 1 August 2005. From that date, numbers where a user is not unambiguously registered will be closed to normal traffic.

PT presupposes that providers will adequately inform their customers in relation to the implementation of these requirements, including contractual matters connected to any closure of traffic to numbers where the customer has a credit typical of pay-as-you-go cards.

Yours faithfully

Willy Jensen

Torstein Olsen

cc.: Norwegian Ministry of Transport and Communications (*Samferdselsdepartementet*)
Norwegian National Authority for Investigation &
Prosecution of Economic and Environmental Crime (*Økokrim*)
Oslo Police District, Organised Crime
The National Police Directorate (*Politidirektoratet*)

The screenshot shows the Swisscom Mobile website interface. At the top left is the logo with the tagline "Go far. Come close." Below the logo is a search bar and a navigation menu with categories like "Home", "New customers", "Private customers", "Subscriptions and tariffs", "NATEL@ budget", "NATEL@ swiss liberty", "NATEL@ international", "NATEL@ pro", "NATEL@ easy", "Purchasing talk time credits", "Registration requirement for prepaid cards", "Numbers with 090 prefixes", "COMBOX@", "Tariff options", "Data communication", "Supplementary services", "Mobile Comfort", "Roaming services", "SMS messaging", "MMS", "E-mailing and internet access", "MMS & SMS Services", "Youth", and "Business customers". The top right features a "Swisscom Group" dropdown menu, "Online-Shop", and "Locations" links. The main content area is titled "Registration requirements for prepaid cards" and contains three sections: "New law requires registration of prepaid cards", "Reactivation", and "Important information regarding registration".

swisscom mobile
Go far. Come close.

Search

Home

- + New customers
- Private customers
 - Subscriptions and tariffs
 - NATEL@ budget
 - NATEL@ swiss liberty
 - NATEL@ international
 - NATEL@ pro
 - NATEL@ easy
 - Purchasing talk time credits
 - Registration requirement for prepaid cards
 - Numbers with 090 prefixes
 - COMBOX@
 - + Tariff options
 - + Data communication
 - + Supplementary services
 - Mobile Comfort - makes phoning easier
 - Roaming services
 - + SMS messaging
 - MMS
 - + E-mailing and internet access
 - + MMS & SMS Services
 - + Youth
 - + Business customers

Swisscom Group Online-Shop Locations

Registration requirements for prepaid cards

New law requires registration of prepaid cards

The Swiss parliament has enacted into law a registration requirement for all users of prepaid SIM cards. The law also requires mobile phone operators to provide their prepaid customers with information regarding these regulations. Therefore, since 1 July 2004 all customers who purchase a prepaid card from Swisscom Mobile must register with Swisscom Mobile.

Customers who made phone calls using NATEL@ easy prior to 1 July 2004 are required to register retroactively. The aim of the law is to prevent fraud and abuse.

Reactivation

In order for you to continue using your mobile phone, you must register at a Swisscom Mobile shop or a post office. Your phone and card will be reactivated within 24 hours, and your phone number and talk time credits will be returned to you.

If you fail to register within a few months following deactivation of your mobile phone, your SIM card will be deactivated, your talk time credits will be invalidated, and your number will be given to another customer.

Important information regarding registration

You must register in person.
Registration is free of charge.
You will be required to present your SIM card and a valid passport or ID card at the post office or Swisscom sales store at which you register.

Annex G: Swisscom Customer Registration Form



Registration for existing NATEL® easy customers

Please register by no later than 31 October 2004. Otherwise we will be required by law to block your NATEL® easy card as of 1 November 2004.

Mandatory details (please complete in full)

- Private customer/
Business customer without extract
from Commercial Register
- Business customer with Commercial Register entry (provide copy)
Public institution

Name

Address

ID type ID card Passport

ID no.

Details of customer/contact person for company/public institution

Last name

First name

Street address

Postcode/city

Country

Date of birth

NATEL® calling number 0 7

Optional information (to help us optimise our service to you)

Ms/Mrs Mr

Language German French Italian English

Phone no. (fixed line) (for questions concerning registration)

Profession

- The customer hereby permits Swisscom Mobile to use these customer details for the purpose of designing and developing services and special offers tailored to customer needs. The customer also agrees to allow these customer details to be processed for the same purposes within the Swisscom Group.

Swisscom Mobile is obliged by law to register customers who started using SIM cards on or after 1 November 2002 and to provide information upon the request of authorities for a minimum period of two years in accordance with the applicable statutory provisions.

The undersigned shall be liable towards Swisscom Mobile for the correctness of the information provided and for any damages which may issue as a result of false, incorrect or insufficient information.

Date

Signature

To be completed by dealer

Information registration >>

Dealer number

Stamp of sales point

