cwta | Association canadienne des télécommunications sans fil
Canadian Wireless Telecommunications Association | acts

October 12, 2007

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

RE: Customer Name and Address Information Consultation

The Canadian Wireless Telecommunications Association ("CWTA") is pleased to provide the following comments to Public Safety Canada in response to the discussion paper on Customer Name and Address information ("CNA"). CWTA is the authority on wireless issues, developments and trends in Canada. It represents cellular, PCS, messaging, mobile radio, fixed wireless and mobile satellite carriers as well as companies that develop and produce products and services for the industry.

CWTA has been actively involved in the consultative discussions about lawful access and related issues since 2002 when Justice Canada issued its first consultation paper regarding this matter. Any new lawful access requirements will ultimately affect the Association's carrier and technology members.

CWTA has consistently advocated for standards-based technical requirements, appropriate compensation for Telecommunications Service Provider ("TSP") costs, and a phased-in approach for the implementation of any newly required technical capabilities. It is the consensus view of our members that the previous legislative proposal, Bill C-74: *Modernization of Investigative Techniques Act*, failed to address those needs.

CWTA strongly urges the government to include concrete measures to address the industry's concerns in any new lawful access legislation. From a practical perspective, unless our legitimate concerns are addressed, it will be difficult for the industry to support this important initiative going forward. Any new requirements must be compatible with the standards-based technology that is available to TSPs.

Canada's telecommunications industry has a long history of working cooperatively with law enforcement within Canada's legal framework for lawful access to communications and access to customer information. While cellular/PCS licencees are the only TSPs that have any legal obligation to provide specific lawful access capabilities within their networks, all carriers have some capability and all carriers respond to law enforcement needs on a routine basis. Canadian TSPs generally, and wireless carriers in particular, maintain dedicated security departments whose sole purpose is to respond to law enforcement requests and comply with court orders. These services are provided at considerable cost to the carriers.

Personal information associated with wireless subscribers is subject to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") rules under the Privacy Commissioner of Canada as well as the *Confidentiality of Customer Information* rules of the CRTC. PIPEDA allows the release of a subscribers' personal information when legally compelled to do so. Unlike wireline telephone numbers, the CRTC considers that wireless telephone numbers are confidential and it requires carriers to treat them as such. CRTC rules allow the release of subscriber's wireless numbers only when carriers are legally compelled to do so.

In order to comply with their obligations under PIPEDA and CRTC rules to protect their customers' privacy, wireless carriers generally require a warrant or court order before providing law enforcement agencies ("LEAs") with confidential customer information. In cases where exigent circumstances or urgent need can be demonstrated, carriers respond to LEAs as quickly and as diligently as possible.

The wireless industry would prefer to continue to provide confidential customer information only subject to court order or warrant except in exigent circumstances. CWTA does, however, agree with Public Safety Canada's observation that there is a lack of clarity for TSPs with respect to the provision of CNA. CWTA would therefore welcome clarification of the scope of CNA and the circumstances and conditions under which TSPs will be compelled to provide CNA to law enforcement. These details should be explicitly identified and clarified in whatever legislation or regulations are enacted.

As mentioned above, wireless carriers maintain dedicated security departments and incur significant costs in order to cooperate and work with LEAs. It is therefore imperative that LEAs compensate TSPs for law enforcement services. This will become even more important if the volume of CNA requests increases under the proposed "no warrant" regime suggested by this consultation. Costs for TSPs to comply will increase substantially along with the increase in requests.

With respect to the specific CNA information under consideration, much of the information listed in the consultation is already available either publicly or via CRTC tariffed services. A variety of third parties provide "reverse look-up" services for Canadian telephone numbers and many of these are provided free of charge on the public Internet. TELUS' LEADS system provides the registered customer's name and the service address of published telephone numbers. Bell's LSPID service provides LEAs with the name of the TSP associated with a 10 digit telephone number. CWTA is not aware of even a single circumstance when law enforcement has demonstrated an inability to obtain CNA information from the wireless industry.

CWTA notes that the types of "basic identifiers" sought for wireless services go well beyond what virtually anyone would consider basic and are much more onerous than those for TSPs using other technologies. IP addresses and dynamic IP addresses, IMSIs, ESNs, IMEIs, and SIM numbers go well beyond basic "tombstone data" normally associated with CNA. For the sake of fairness, consistency, competitive equity, and technological neutrality, wireless carriers should not be compelled to provide greater levels of information than other TSPs.

If the government does take action to define TSP obligations with respect to CNA, it should clearly recognize the limits of TSPs' ability to respond in a timely manner. Given that certain wireless CNA information has always been considered confidential, systems that can provide quick response for directory assistance have never been developed for wireless services. Wireless carriers work diligently to respond to LEA requests, but face constraints on their ability to provide information. These limitations may be a result of the volume of requests, the details required, or other factors, but it should be recognized in whatever requirements may be imposed that TSPs cannot always respond as quickly as may be desired.

CWTA further notes that wireless carriers do not always have any business reason to collect customer information, and so do not have verified CNA data in their possession in all circumstances. As you will

recall, CWTA addressed this in its comments to the Department of Justice Canada dated December 16, 2002:

> The CWTA strongly opposes the imposition of [a provision of subscriber or service provider information] obligation beyond those situations where a wireless carrier is already collecting this information. Moreover, the CWTA is of the view that service providers should not be liable for the accuracy of customer name and/or address information. In this regard, the CWTA would note that the European Convention refers to subscriber information in that service provider's possession or control.
>
> Generally, wireless carriers collect, validate and maintain customer information to the extent that such information is necessary to successfully provide service and to collect payment. For postpaid services (services for which the customer receives a monthly bill), wireless carriers would typically undertake a credit check to determine a prospective customer's ability to make monthly payments for the services provided. However, this process is geared to validating credit worthiness, not customer name and address. Wireless carriers do not undertake exhaustive validation of the information that is provided by customers and wireless carriers do not warrant that such information is valid or correct, or that it would satisfy the requirements of law enforcement and security agencies. Further, wireless carriers are almost entirely reliant on customer initiated notification with respect to address changes.
>
> Consequently, the CWTA opposes the imposition of any obligation for service providers to collect information that they are not already collecting for their own purposes. Significant service, business and cost issues would arise if wireless carriers were required to collect, validate and maintain accurate customer information for the purposes of lawful access.
>
> First, any such requirement would likely obligate wireless carriers to insist that customers present a minimum degree of official identification at the point of purchase. This would also require that wireless carriers, and the literally thousands of independent distribution agents and outlets they rely on, would be capable of validating such identification. CWTA notes in this regard the concerns raised by the Privacy Commissioner of Canada.
>
> Second, an overwhelming issue arises with respect to on-line purchases of a wireless service since, for these purchases, the entire transaction is conducted over the Internet, not in person. Similarly, customers who opt for on-line billing will be billed on-line and will not have a monthly invoice sent to a physical address. If they chose to move, the carrier will have not means of knowing, apart from the customer taking the initiative to update this information by accessing their on-line account. In the case of purchasing or billing, on-line transactions do not lend themselves to the presentation and validation of the customer's identification. Wireless carriers, and countless other businesses in Canada and abroad, have already made significant investments in on-line purchasing, billing and customer relations capabilities and they rely on this channel as a useful and cost-effective means by which to acquire, bill and interface with their customers.
>
> Third, another 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 the information.
>
> It should be noted that this situation is not isolated to wireless phones. The verification of a customer's address is only necessary when a service provider must establish a physical connection to the customer. For example; Direct Broadcast Satellite, Multipoint Distribution Service, dial-up Internet Service Providers, and prepaid local and long distance phone card providers are also capable of providing service without knowing the address of the customer.

All of the foregoing remains true today, and CWTA continues to oppose any obligation that would require TSPs to collect customer information beyond what is already collected for business purposes.

Conclusion

The CWTA recognizes that lawful access to communications and the ability to obtain CNA information are important tools for law enforcement. To function properly, however Canada's lawful access regime must recognize the realities of the telecommunications industry:

- TSPs must be compensated for the significant costs incurred responding to the requirements of LEAs.
- Any new technical requirements must be based on international standards, and provide an adequate phase-in period.
- The scope of CNA information and the circumstances under which it would be provided by TSPs to law enforcement should be explicitly identified and clarified in whatever legislation or regulations are enacted.
- CNA requirements should be applied in a technologically and competitively neutral fashion.
- TSPs should not be required to collect customer information beyond what is already collected for business purposes.

CWTA appreciates the opportunity to provide these comments. Given that there are no proposals in this consultation, CWTA requests the opportunity to comment on any changes the government intends to make to the current lawful access regime.

CWTA believes that the importance of this matter warrants full disclosure of the issues involved and encourages the Department to make all comments received through this consultation public. CWTA will be posting these comments on the Association's website.

Sincerely,

Filed electronically

J. David Farnes
Vice President,
Industry and Regulatory Affairs