August 22, 2012

Mr. John Macri
Director, Telecommunications Policy
Canadian Radio-television and Telecommunications Commission
1 Promenade du Portage
Gatineau (Québec) K1A 0N2

Dear Mr. Macri:

RE: CWTA reply to CRTC's August 8th 2012 letter re: Privacy concerns due to the unmasking of blocked Caller ID information

1. The Canadian Wireless Telecommunications Association (CWTA) is the authority on wireless issues, developments and trends in Canada. It represents wireless service providers, as well as companies that develop and produce products and services for the industry.

2. CWTA is in receipt of the Commission's letter dated August 8th, 2012, sent to several CWTA members requesting information relating to third-party applications that would allow Canadian wireless subscribers to unmask telephone numbers that have been blocked using the Caller ID blocking feature. As an example, the Commission noted that the TrapCall service, which is provided by Teltech Systems, allows a user to unmask a telephone number that has been blocked using the Caller ID blocking feature.

3. Specifically, the Commission's letter requests that Canadian wireless carriers respond to the following questions:

    i. Are you aware of any applications or services, such as TrapCall, available to your subscribers that have the ability to circumvent privacy safeguards? If so, please identify these services and describe how they work.
    ii. Have you received any customer complaints with respect to the TrapCall service or similar services that circumvent privacy safeguards? If so, please provide the nature and number of complaints received.
    iii. Describe the actions, if any, that you have taken or that you propose to take to address the potential violation of subscribers' privacy expectations.

T 613 233 4888 F 613 233 2032 www.cwta.ca
1110-130 rue Albert Street Ottawa, ON K1P 5G4

a) Provide a description of each technical solution and explain, with supporting rationale, which solution would be most effective in addressing the issue of circumventing the Caller ID blocking feature.

b) Identify and explain any other potential approaches, such as regulatory measures or changes in your company's terms of service, that can be implemented to maintain the privacy expectations of subscribers.

4. Like Commission staff, the CWTA and its members believe that the protection of subscribers' privacy is a fundamental telecommunications policy objective. As such, I am pleased to provide the following response on behalf of the CWTA members that received your letter.

Caller ID unmasking applications and services

5. Preliminary research has revealed a number of existing services or applications that appear to be similar to TrapCall. While we cannot speculate specifically on how every privacy-circumventing service works, we can provide the following general overview of a how caller-ID block circumvention takes place:

6. Caller-ID unmasking relies on the features inherent to Signaling System Number 7 (SS7). SS7 is a set of telephony signaling protocols developed in 1980 by the CCCIT/ITU-T to set up the majority of global public switched network telephone calls. SS7 was never intended to be accessed by non-carriers. Proper routing and carriage of flags such as 'caller-ID block' requires each carrier in the communication string to respect the protocol and accurately carry forward call information, including flags. Canadian carriers abide by the CRTC's rules regarding routing and carrying privacy flags. However, the development of Voice over IP and cheaper PBX equipment allows non-carriers to access, and in turn manipulate, SS7 information.

7. In a TrapCall use scenario, when the called party (the TrapCall user) has downloaded the TrapCall app to their phone, Call Forwarding on the TrapCall user's phone will forward incoming calls to TrapCall's non-carrier, SS7 capable equipment, such as an IP-PBX device or server. The equipment receives the forwarded call, turns off the caller-ID blocking flag in the SS7 signalling, and then routes the call back to the TrapCall user. The previously-blocked caller-ID is then displayed on the screen of the called party's phone.

8. Caller-ID blocked calls can also be forwarded to a US toll-free 800 number where, under FCC regulations, blocked private information can be displayed in order to allow the carrier to forward billing information to the 1-800 customer. That information could then

be forwarded by the 1-800 customer to the TrapCall (or other Caller-ID circumvention service) user, whose subsequent use of the number would violate FCC rules.[1]

9. It is important to note the following additional details about TrapCall and similar circumvention services:

   i. The caller and the carrier have no absolutely no visibility into what is going on during the use of TrapCall or similar circumvention services. The event is in the control of the called party and the circumvention service, and occurs entirely outside the scope of carrier involvement, equipment, or control.
   ii. Caller-ID blocking can be unmasked on both wireless and wireline calls.
   iii. This is a global issue, as the call forwarding may cross borders, and the service may operate from another country.
   iv. Increased availability, and decreased prices, of telecom equipment such as VoIP, soft phones, soft switches and PBX devices have amplified the risk of circumvention services and applications.

Customer complaints

10. CWTA members collectively have received fewer than ten total inquiries about TrapCall or similar circumvention services. Most inquiries, from customers and law enforcement officials, have focused on the availability, or lack thereof, of the service. This is not surprising as callers are unlikely to know if their caller-ID was unblocked through the use of a circumvention service unless they were so informed by the party using the service. Nevertheless, CWTA and its members take these inquiries seriously and continue to work with partners to explore potential solutions to these and other SS7 signaling exploits.

11. CWTA members generally have terms of service that prevent users of telecommunications services from interfering with a communication, or invading or violating an individual's privacy, which CWTA believes would encompass interference with any call information including privacy flags, conveyed through SS7 signaling. However, as mentioned above, neither CWTA members nor the calling party would be aware of manipulations initiated by the called party using a circumvention service such as TrapCall. It should be noted that circumvention services themselves are not a contracting party with wireless carriers – only the customer is. As a result, CWTA members are not in a position to enforce their Terms of Service against circumvention services directly.

Solutions

[1] FCC, Guide to Caller ID and Spoofing. http://www.fcc.gov/guides/caller-id-and-spoofing

12. As the Commission is aware, Teltech stopped offering the TrapCall service in Canada in May 2012. However, the members of CWTA believe that this issue warrants further consideration through an existing channel for investigation, either CISC-Emergency Services Working Group (ESWG), and/or the Office of the Privacy Commissioner (OPC).

13. CWTA notes that carrier personnel investigating circumvention services are also currently involved in CISC- ESWG's discussions on "caller-ID spoofing" in the context of 911, which is also based on exploiting vulnerabilities associated with SS7 signalling (Coincidentally, Teltech also offers a caller-ID spoofing service called SpoofCard). Given the public safety considerations associated with circumventing caller-ID blocking (particularly for law enforcement and residents of shelters for victims of domestic violence), CWTA submits that the current agenda for CISC-ESWG Task Identification Forum be expanded to consider caller-ID unblocking. It is worth noting that a signalling-based solution could interfere with legitimate caller-ID and call forwarding and may take years to deploy through network upgrades.

14. In addition, as circumvention services are disclosing information independent of carrier involvement, such services could be more efficiently investigated by the OPC. The OPC has indicated that it would be a breach of the *Personal Information Protection and Electronic Documents Act* to display the name and number of a customer using caller-ID blocking to a called party, without that customer's knowledge and consent.[2]

15. Therefore, while a CRTC-based solution would likely involve pursuing the non-carrier offenders indirectly through carriers (which would have inherent limitations and challenges outlined above) the OPC could directly pursue the offending parties under existing legislation.

Conclusion

16. CWTA recognizes that although TrapCall is not currently available in Canada, the availability and low cost of the necessary equipment all but ensure that more privacy-circumventing services will materialize and need to be addressed in the future.

17. CWTA and its members is committed to protecting the privacy of all telecommunications service users, and support the investigation of appropriate methods of addressing the privacy issues that arise as a result of circumvention services such as TrapCall.

[2] PIPEDA Case Summary #2002-75. http://www.priv.gc.ca/cf-dc/2002/cf-dc_021010_1_e.asp.

18. Given the nature of these services, the ways in which they operate, and the fact that wireless carriers are not able to detect when these services are being used, CWTA respectfully submits that the appropriate way forward at this stage involves reference of this issue to CISC-ESWG (which is examining directly-related issues) and/or the OPC (which has the tools to pursue the offending parties directly under PIPEDA).

Sincerely,

Jim Patrick
Senior Vice President

Cc: William Lloyd, william.lloyd@crtc.gc.ca
James Ndirangu, james.ndirangu@crtc.gc.ca