TekSavvy Solutions Inc.
Privacy Ombudsman
800 Richmond Street
Chatham, Ontario N7M 5J5

January 20, 2014

Dear TekSavvy Solutions Inc. Privacy Ombudsman:

We are academic researchers and civil rights organizations who investigate Canadian privacy, security, and speech issues, often as they relate to telecommunications practices and networks. Given the importance of such communications to the Canadian political and economic matters, it is imperative that Canadians have trust and confidence that their digital communications are treated with dignity and are protected from undue access, collection, retention, analysis, or disclosure by third-parties.

Given the importance of communications for Canadians, we are sending this letter to your company and the country's other major telecommunications carriers to ask about your data retention and sharing policies. Specifically, we are asking how, when, and why your company discloses information to government agencies. Your responses are needed to make informed public policy decisions about how best to protect Canadians' security as well as their privacy, and the responses given will be made public. For each question, please provide either a response, indicate that you cannot respond, or indicate that you will not respond.

1. In 2012 and in 2013, how many total requests did your company receive from government agencies to provide information about your customers' usage of communications devices and services:
    a. Within that total, please list the amount of requests your company received for <u>each</u> type of usage, including but not limited to: 1) Geolocation of device (please

distinguish between real-time and historical); 2) Call detail records (as obtained by number recorders or by disclosure of stored data); 3) Text message content; 4) Voicemail; 5) Cell tower logs; 6) Real-time interception of communications (i.e. wiretapping); 7) Subscriber information; 8) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.); 9) Data requests (e.g. web sites visited, IP address logs); 10) Any other kinds of data requests pertaining to the operation of your network and business.

   b. For each of the request types, please detail all of the data fields that are disclosed as part of responding to a request.
   c. Within the aforementioned total, how many of the requests were made for real-time disclosures, and how many were made retroactively for stored data?
   d. Within the aforementioned total, how many of the requests were made in exigent circumstances, and how many were made in non-exigent circumstances?
   e. Within the total, how many of the requests were made subject to a court order?
   f. Within the total, how many of the requests did your company fulfill and how many did it deny? If your company denied requests, for what reasons did it do so?
   g. Within the total, please identify how many requests were made by Federal, by provincial, and by municipal government agencies.
   h. Do you notify your customers when government agencies request their personal information? If so, how many customers per year have you notified?

2. For <u>each</u> type of usage in 1(a), how long does your company retain those records and the data fields associated with them?
3. What is the average amount of time law enforcement requests for each of the information requests in 1(a) (e.g. 3-5 days of records)? What is the average amount of time that your company is typically provided to fulfill each of the information requests in 1(a)?
4. How many times were you asked to disclose information noted in 1(a) based specifically on:
   a. child exploitation grounds?
   b. terrorism grounds?
   c. national security grounds?
   d. foreign intelligence grounds?
5. What protocol or policies does your company use to respond to requests for data that are noted in 1(a)?
   a. What legal standard do you require government agencies to meet for <u>each</u> type of data request noted in 1(a)?
   b. What are the average number of subscribers who typically have their information disclosed in government agencies requests, for <u>each</u> type of request noted in 1(a)?
   c. Does your company have distinct policies to respond to exigent and non-exigent requests? If yes, what are these policies or how do they differ?

    d. Is your company required to design your networks and services so government agencies can more readily access customer data in a real time or in a retroactive manner? If yes, please detail those requirements.
    e. Does your company have a dedicated group for responding to data requests from government agents? Are members of this group required to have special clearances in order to process such requests? What is the highest level company official that has direct and detailed knowledge of the activities of this group?
6. What is the maximum number of subscribers that the government requires you to be able to monitor for government agencies' purposes, for each of the information types identified in 1(a)? Have you ever received an official order (e.g. ministerial authorization, court order, etc.) to expand one of those maximum numbers?
7. Has your company received inappropriate requests for information identified in 1(a)? If yes, why were such requests identified as inappropriate and who makes a decision that a request is inappropriate? And if yes, how did your company respond?
8. Does your company have any knowledge of government agencies using their own:
    a. tracking products (e.g. 'IMSI Catchers')?
    b. infiltration software (e.g. zero day exploits, malware, such as FinFisher, etc.)?
    c. interception hardware (i.e. placed within or integrated with your company's network)?
    d. If yes to 8(a), (b), or (c), please explain.
9. Does your company cooperate with government agencies that use their own tracking equipment or provide information on how to interoperate with your company's network and associated information and subscriber information? If yes, how does it cooperate, how many requests does it receive for such cooperation, and how many of your subscribers have been affected by such equipment or interoperation?
10. In 2012 and 2013, did your company receive money or other forms of compensation in exchange for providing information to government agencies? If yes, how much money did your company receive? And if yes, how much does your company typically charge for specific services (please refer to the list in 1(a) above)?
    a. Does your company charge different amounts depending on whether the request is exigent or non-exigent? Does your company charge fees for exigent cell phone tracking requests from law enforcement authorities?
    b. Please include any written schedule of fees that your company charges law enforcement for these services.
    c. Does your company operate purely on a cost recovery basis for providing information to government agencies?

Thank you for your attention to this important matter. Please provide a response, or commitment to respond, to these questions by March 3, 2014. If you have any questions please contact, or

have a member of your staff contact, Christopher Parsons at christopher@christopher-parsons.com.

Sincerely,

Lisa Austin
Associate Professor, Faculty of Law at University of Toronto

Colin Bennett
Professor, Department of Political Science at University of Victoria

Andrew Clement
Professor, Faculty of Information at University of Toronto

Ron Deibert
Director, the Citizen Lab and the Canada Centre for Global Security Studies, Munk School of Global Affairs at University of Toronto

Robert Diab
Law Professor, Faculty of Law at Thompson Rivers University

Michael Geist
Canada Research Chair in Internet and E-commerce Law, Faculty of Law at University of Ottawa

Adam Molnar
Postdoctoral Fellow, the Surveillance Studies Centre at Queen's University

Christopher Parsons
Postdoctoral Fellow, the Citizen Lab, Munk School of Global Affairs at University of Toronto

Andrea Slane
Associate Professor, Faculty of Social Sciences and Humanities at University of Ontario

Valerie Steeves
Assistant Professor, Department of Criminology at University of Ottawa

Kevin Walby
Assistant Professor, Department of Criminal Justice at University of Winnipeg

Dwayne Winseck
Professor, School of Journalism and Communication and Institute of Political Economy at Carleton University