Lawful Interception of Communication by Security and Intelligence Organizations: The Policy and Legal Challenges Posed By Real-Time Messaging on Internet Platforms

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

May 2024

Executive Summary

Canadian lawful access public policy has long sought to ensure that law enforcement and intelligence agencies have appropriate access to information for investigative purposes while ensuring that privacy and due process is fully respected. The legal and policy debate has largely envisioned communications that place Canadian communications companies – telecom, wireless and Internet providers – at the centre of the communication chain. The Supreme Court's privacy jurisprudence has steadily eroded the policy justifications for warrantless access to Internet user information collected and retained by those companies. That has shifted the burden to law enforcement, who typically must now obtain a court order to obtain the access to the desired information. Yet alongside the shift in the law on the reasonable expectation of privacy, a second development has transformed the relative importance of lawful access policy: the emergence of Internet-based messaging services that render law enforcement access even more challenging.

The Internet landscape of messaging and social media services is constantly evolving with new services attracting hundreds of millions of users and challenging the established leaders. This report covers the largest services, some with billions of users worldwide. The research for each company involved several components. First, a comprehensive review of all publicly-available policies, including information related to data collection and retention, encryption, law enforcement request responses, applicable laws, and evidentiary standards. Second, an analysis of publicly-available transparency reports for each company where available. Third, a caselaw and secondary source review was conducted to identify relevant cases or other publicly available information.

Among these services, the report first reviews four leading messaging services: WhatsApp, Signal, Telegram and Viber. The primary takeaway with respect to these services is that most content is not stored on company servers and the use of encryption further limits potential access to the content of user messages. The companies may be able to provide non-content information regarding subscribers, subject to a court-supervised disclosure process.

Three social media services with messaging functionality are then covered: X (formerly Twitter), TikTok, and Snap. The difference between a social media service with messaging and a messaging service becomes immediately apparent. Unlike messaging services that do not retain content or deploy encryption limiting access, these social media services typically retain far more content-based information, including as part of their messaging functionality. The companies therefore face far more law enforcement request for customer information, maintain more robust policies, and address issues such as data retention and privacy compliance.

Finally, the report also reviews the three largest tech giants that also offer messaging or email functionality: Google, Apple, and Microsoft. The primary difference between tech giants and social media services with messaging functionality is the breadth of data collected by the giants.

The report identifies six key issues that should be the core focus for operational analysis or future policy development in light of the essential role played by the messaging services. These include: the challenges of messaging-only apps, the limits of mandated data disclosures, jurisdictional challenges, inconsistent policies, encryption, and uncertainty and transparency.

Introduction

Canadian lawful access public policy has long sought to ensure that law enforcement and intelligence agencies have appropriate access to information for investigative purposes while ensuring that privacy and due process is fully respected. The legal and policy debate has largely envisioned communications that place Canadian communications companies – telecom, wireless and Internet providers – at the centre of the communication chain. Prior to the Supreme Court of Canada decision in *Spencer,* the policies adopted by these providers typically governed the disclosure process, including under what circumstances data would be provided, under what conditions, and subject to what timelines.

In recent years, the communications chain has expanded dramatically with these telecommunications providers still providing the means of network access, but playing a diminished role in the content of the communications themselves. That often means that the providers may be positioned to confirm details related to access, but with limited visibility into information about much else. Rather, Internet platforms and real-time communications services have assumed the critical role in facilitating network-enabled communications with services that include synchronous and asynchronous chat and messaging. These companies are rarely Canadian-based, deploy varying degrees of encryption, may establish differing standards for law enforcement disclosure, and frequently issue expansive transparency reports.

This research report will provide a starting point for developing policy with respect to these services. The report is divided into three parts. Part one provides a backgrounder on lawful access and the policy debate that raged in Canada for the better part of two decades. Part two identifies the key messaging services, divided into three groups of services: messaging services, social media services with messaging functionality, and tech giants. Part three discusses recommendations for policy reform and engagement based on the earlier analysis. The report also includes an appendix with specific data for each company across a series of metrics, including government and law enforcement requests, request processes, request types, customer data, retention policies, and encryption practices.

I. Background

1. Lawful Access Legislative Proposals

The push for new Internet surveillance capabilities dates back to 1999, when government officials began crafting proposals to institute new surveillance technologies within Canadian networks along with additional legal powers to access surveillance and subscriber information. A bill introduced in 2010 contained a three-pronged approach focused on information disclosure, mandated surveillance technologies, and new police powers. For the purposes of this report, it is the first prong, which mandated the disclosure of Internet provider customer information without court oversight, that is most relevant. Under privacy law at the time, providers could voluntarily disclose customer information but were not required to do so. The new system would have required the disclosure of customer name, address, phone number, email address, Internet protocol address, and a series of device identification numbers.

While some of that information may have seemed relatively harmless, the fear was that the ability to link it with other data would often open the door to a detailed profile about an identifiable person. Given its potential sensitivity, the decision to require disclosure without any oversight raised concerns within the Canadian privacy community.

That bill stalled, but in February 2012, then-Public Safety Minister Vic Toews introduced Internet surveillance legislation that once again sparked widespread criticism from across the political spectrum. The overwhelming negative publicity pressured the government to quickly backtrack by placing it on hold. In 2013, then-Justice Minister Rob Nicholson announced that the bill was dead, confirming "we will not be proceeding with Bill C-30 and any attempts that we will continue to have to modernize the Criminal Code will not contain the measures contained in C-30."[1]

Nicholson's commitment lasted less than a year. By 2014, Peter MacKay, then the new federal justice minister, unveiled Bill C-13, which was marketed as an effort to crack down on cyber-bullying. Yet the vast majority of the bill brought back many (though not all) lawful access provisions found in the earlier proposal. For example, the bill encouraged telecom companies and Internet providers to reveal information about their customers to law enforcement without a court order by granting them immunity from criminal or civil liability for such disclosures.

2. Spencer

While government was introducing successive lawful access proposals, the Supreme Court of Canada was steadily eroding the foundation behind the policy by strengthening privacy protections. For example, despite claims that metadata carried little privacy interest, the Court ruled in *R. v. Vu* that "in the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly."[2]

More notably, in 2014, the Court issued its decision *R. v. Spencer*,[3] which largely ended the debate over whether there is a reasonable expectation of privacy in basic subscriber information. First, the Court recognized that there is a privacy interest in subscriber information. While the government had consistently sought to downplay that interest, the court found that the information is much more than a simple name and address, particular in the context of the Internet. As the court states:

the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users. Browsing logs, for example, may provide detailed information about users' interests. Search engines may gather records of users' search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns. Cookies may be used to track consumer habits and may provide information about the options selected within a website, which web pages were visited before and after the visit to the host website and any other personal information provided. The user cannot fully control or even

[1] https://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384
[2] 2013 SCC 60.
[3] 2014 SCC 43.

necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous – by guarding the link between the information and the identity of the person to whom it relates – the user can in large measure be assured that the activity remains private.[4]

Given all of this information, the privacy interest is about much more than just name and address.

Second, the court expanded the notion of informational privacy, concluding that there are three conceptually distinct issues: privacy as secrecy, privacy as control, and privacy as anonymity. It is anonymity that is particularly notable as the court recognized its importance within the context of Internet usage. Given the importance of the information and the ability to link anonymous Internet activities with an identifiable person, a high level of informational privacy is at stake.

Third, not only is there a significant privacy interest, but the court concluded that there is also a reasonable expectation of privacy by the user. The court examines both PIPEDA and the Shaw terms of use (the Internet provider in the case) and concluded that PIPEDA must be understood within the context of protecting privacy and that the ISP agreement was confusing at best and may support the expectation of privacy. With those findings in mind it stated:

in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.[5]

Fourth, having concluded that obtaining subscriber information was a search with a reasonable expectation of privacy, the information was unconstitutionally obtained which therefore led to an unlawful search. Addressing the impact of the PIPEDA voluntary disclosure clause, which was commonly used by Internet providers at the time, the court noted:

Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, I do not see how they could gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information.[6]

The decision sparked significant reform among Internet providers in their approach to the disclosure of subscriber information. Indeed, the Supreme Court examined Shaw's terms of service policy and found it provided "a confusing and unclear picture of what Shaw would do when faced with a police request for subscriber information." While providers had been regularly disclosing this information hundreds of thousands of times, the Court ruled:

Given that the purpose of PIPEDA is to establish rules governing, among other things, disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information (s. 3), it would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal

[4] Ibid. at para 46.
[5] Ibid. at para 66.
[6] Ibid. at para. 73.

information or defeat PIPEDA's general prohibition on the disclosure of personal information without consent.[7]

The court noted that ISPs were not required to disclose this information and the case reached the conclusion that they were not permitted to do so absent a warrant either.

3. Bykovets

The Spencer ruling addressed the reasonable expectation of privacy associated with basic subscriber information. The Supreme Court expanded its analysis in 2024 by considering the privacy expectations of IP addresses in *R. v. Bykovets*.[8] IP addresses, which are a string of numbers that link to a specific Internet location, would previously have been viewed to have an even weaker privacy interest than subscriber information. However, the court ruled that it too carried a reasonable expectation of privacy, emphasizing how the IP address can be used to link to other personal information:

Casting the subject matter of this search as an abstract string of numbers used solely to obtain a Spencer warrant goes against these precedents. IP addresses are not just meaningless numbers. Rather, as the link that connects Internet activity to a specific location, IP addresses may betray deeply personal information — including the identity of the device's user — without ever triggering a warrant requirement. The specific online activity associated with the state's search can itself tend to reveal highly private information. Correlated with other online information associated with that IP address, such as that volunteered by private companies or otherwise collected by the state, an IP address can reveal a range of highly personal online activity. And when associated with the profiles created and maintained by private third parties, the privacy risks associated with IP addresses rise exponentially. The information collected, aggregated and analyzed by these third parties lets them catalogue our most intimate biographical information. Viewed normatively and in context, an IP address is the first digital breadcrumb that can lead the state on the trail of an individual's Internet activity. It may betray personal information long before a Spencer warrant is sought.[9]

In light of that analysis, the Court concluded that it too requires a warrant:

As a crucial component inherent in the structure of the Internet, an IP address is the key that can lead the state through the maze of a user's Internet activity and is the link through which intermediaries can volunteer that user's information to the state. Thus, s. 8 ought to protect IP addresses. Doing so would safeguard the first "digital breadcrumb" and shroud the trail of an Internet user's journey through cyberspace; it would further s. 8's purpose of preventing potential infringements of privacy rather than circumscribe its scope according to the state's stated intentions about how it will use this key[10].

While the full effect of *Bykovets* has yet to unfold, it seems likely to further limit warrantless access to Internet information to be disclosed by telecom and Internet companies.

---

[7] Ibid. at para. 62.
[8] 2024 SCC 6.
[9] Ibid. at para 9.
[10] Ibid. at para 13.

The Supreme Court's privacy jurisprudence has steadily eroded the policy justifications for warrantless access to Internet user information collected and retained by Internet and telecommunications companies. That has shifted the burden to law enforcement, who must now typically obtain a court order to obtain the access to the desired information. Yet alongside the shift in the law on the reasonable expectation of privacy, a second development has transformed the relative importance of lawful access policy: the emergence of Internet-based messaging services that may render law enforcement access even more challenging.

II. Messaging and Social Media Services Policies

The Internet landscape of messaging and social media services is constantly evolving with new services attracting hundreds of millions of users and challenging the established leaders. This survey covers the largest services, some with billions of users worldwide. While the initial proposal for this study was largely limited to services such as Twitter (now X), Snap, WhatsApp, Signal, and Viber, further research revealed that this group of services failed to fully capture the full scope of the market and the challenges faced by law enforcement and government authorities in seeking access to communication information in a similar fashion to lawful access with domestic communications companies. The research was therefore significantly expanded with the removal of one service (Slack, which did not neatly fit within the messaging and social media paradigm as an in-house messaging service) and the inclusion of a far broader range of services including Telegram, Snap, TikTok, Google, Apple, and Microsoft.

The research for each company involved several components. First, a comprehensive review of all publicly-available policies, including information related to data collection and retention, encryption, law enforcement request responses, applicable laws, and evidentiary standards. Second, an analysis of publicly-available transparency reports for each company where available. These reports provide further information on how policies are operationalized as well as aggregated data on requests and responses. In some instances, the data is specific to Canada. Third, a caselaw and secondary source review was conducted to identify relevant cases or other publicly available information. This review identified some relevant cases and media reports, notably including a Quebec decision involving Snap that specifically grappled with the issues relevant to this study. All data is current to data released by January 2024, though the actual data may refer to practices that date back to 2021-2022.

The results of this research is presented below on a company-by-company basis grouped into three categories: messaging services, social media services with messaging functionality, and tech giants, which refers to Apple, Google, and Microsoft, each of which maintain messaging services as part of a much-larger array of products and services. An appendix to this report features the raw data compiled during the research phase.

i. Messaging Services

This section reviews four leading messaging services: WhatsApp, Signal, Telegram and Viber. Collectively, the services have billions of users. The primary takeaway with respect to these services is that most content is not stored on company servers and the use of encryption further

limits potential access to the content of user messages. The companies may be able to provide non-content information regarding subscribers, subject to a court-supervised disclosure process.

1. *WhatsApp*[11]

WhatsApp is the world's most popular messaging service. Purchased by Meta (then Facebook) in 2014, the service currently has roughly 3 billion users. WhatsApp cannot and does not produce the content of its users' messages in response to government requests. The content of all messages sent using WhatsApp are protected by an encryption protocol that secures messages before they leaving a user's device, which ensures that only the user and the recipient can listen or read the message. This removes access for intermediaries, including WhatsApp itself.

While content cannot be disclosed, WhatsApp discloses basic subscriber information such as name, service start date, last seen date, IP address, device type, and email address. Moreover, account information such as a user's "about" information, profile photos, group information and contacts list is retained by the company and subject to potential disclosure. In order to comply with legal requests, once approved Whatsapp records messages, call logs for a particular user indicating who the communication was to or from, the time it was transmitted and from which IP address, and the type of communication (such as a text or call).

Whatsapp publishes requests and responses twice a year in Meta's Government Requests for Data Report. This is a global report. In the first six months of 2022, Canadian authorities sent 1,149 legal requests to Whatsapp as well as an additional 1,710 emergency disclosure requests. These requests implicated 4,150 user account were requested with 83.70% of requests producing some data.[12]

WhatsApp maintains a dedicated, trained Law Enforcement Response Team (LERT) that reviews and evaluates each government request for user data, whether the request was submitted related to an emergency or as part of a legal process initiated by law enforcement or government authorities. In reaching a decision on disclosures, WhatsApp considers applicable law, internationally recognized standards such as human rights, due process, and the rule of law. A mutual legal assistance treaty request or letters rogatory may be required for international requests. In the event of a disclosure, users are notified of the disclosure, except in cases involving child exploitation and emergency threat to life. WhatsApp may preserve customer data in response to a valid preservation request, but it has not publicly disclosed the time period for preservation.

2. *Signal*[13]

Signal is an encrypted messaging service. First established in 2010, it is now maintained by the Signal Foundation, which was supported by Brian Acton, the co-founder of WhatsApp. As of 2022, Signal was estimated to have 40 million users worldwide.

---

[11] https://faq.whatsapp.com/808280033839222
[12] https://transparency.fb.com/data/government-data-requests/country/CA/
[13] https://signal.org/legal/

Signal uses an end-to-end encryption by default model, which means that messages are not stored. It is therefore unable to access virtually any details about its users including messages, chat lists, groups, contacts or even profile names. It does not report on lawful access requests, maintaining that is unable to comply with such requests.

While it does not provide content related data, Signal will provide non-content data such as the date of registration and date of most recent connection to the Signal servers, upon receipt of a valid court order.

3. *Telegram*[14]

Telegram was launched in 2013 by two Russian brothers, who previously founded VK, a Russian social media service. The company is now registered in the British Virgin Islands and as a limited liability company in Dubai. The service has 900 million users and has been considering filing to become a public company.[15]

Telegram offers two main types of messages, both of which are encrypted but which differ with respect to potential company access. First, cloud chats are stored on Telegram servers. Telegram holds the encryption keys in a different physical location and jurisdiction from where the encrypted message is stored. Second, secret chats are encrypted using a key which is only known to the sender and recipient. Secret chats are not stored on Telegram servers.

Telegram is able to access the following user data:

- Phone number
- Profile name (which does not have to be real name)
- Profile photo
- "About" info on profile
- Email address, if used for two-factor authentication
- Location data, if shared in a cloud chat

Telegram maintains that it will only disclose user information under a court involving suspicion that the user is a terror suspect. While the company insists that has never released customer data, a 2022 Der Spiegel report claims Telegram has shared data with German police in cases of child abuse and terrorism.[16]

4. *Viber*[17]

[14] https://telegram.org/privacy?setln=it
[15] https://www.ft.com/content/8d6ceb0d-4cdb-4165-bdfa-4b95b3e07b2a
[16] https://www.spiegel.de/netzwelt/apps/telegram-gibt-nutzerdaten-an-das-bundeskriminalamt-a-0e4d3fcb-8081-4b87-b062-db412bbc294b
[17] https://www.viber.com/en/terms/viber-public-content-policy/#:~:text=Respect%20the%20Law%20and%20Our,illegal%20drugs%2C%20goods%20or%20services

Viber is an instant messaging and voice service originally founded in Israel and owned since 2014 by Rakuten, a Japanese company. The service has an estimated 1.3 billion users and is particularly popular in Eastern European countries.

Company access to content data is limited to undelivered messages. Otherwise, content data is end-to-end encrypted and cannot be decrypted by Viber. It is only decrypted by the sender and the recipient. Viber may disclose customer data to law enforcement in response to requests relating to activity which may expose Viber or the customer to legal liability. The company discloses information to law enforcement, governmental agencies, or authorized third-parties, in response to a verified request relating to terror acts, criminal investigations or alleged illegal activity or any other activity. Non-content data held by the company includes:

- Mobile phone number
- Name
- Email address
- Contacts list
- IP address
- Device identifiers

Viber policy indicates that it notifies users regarding the submission of a law enforcement request prior to the disclosure of any account records, except where: (i) providing notice is prohibited under applicable regulation, court order, subpoena or other legal process; (ii) emergency event occurs and providing a notice could result in a significant risk (e.g., injury or death) to an individual or a group of individuals; or (iii) an emergency event involves potential harm to minors. Viber will honour preservation requests for 90 days, and will accept extension requests for one additional 90 day period.

ii. Social Media Services With Messaging Functionality

Three social media services with messaging functionality are covered in this section: X (formerly Twitter), TikTok, and Snap. These enormously popular services are not focused on person-to-person messaging, but it is offered on each service. The difference between a social media service with messaging and a messaging service becomes immediately apparent upon review of the data. Unlike messaging services that do not retain content or deploy encryption limiting access, these social media services typically retain far more content-based information, including as part of their messaging functionality. The companies therefore face far more law enforcement request for customer information, maintain more robust policies, and address issues such as data retention and privacy compliance.

1. X (formerly Twitter)[18]

X, formerly known as Twitter, is a popular micro-blogging social media service. Currently owned by Elon Musk, the service has undergone dramatic shifts with the changes in ownership such that some of the company's policies may no longer fully reflect corporate practices. The

[18] https://help.twitter.com/en/rules-and-policies/x-law-enforcement-support

service currently has over 500 million active users. Twitter publishes reports of all the legal requests it receives twice a year.[19]

Non-content data held by the company includes:

- Display name
- Username
- Email
- Phone number
- Payment methods
- IP address

Content data includes:

- Tweets
- Images
- Direct messages

X follows industry best-practices of encrypting data at rest and in transit. X apps must use encryption to connect to the X API.

X considers legal requests for customer data when those requests have a valid legal basis. It considers emergency requests in situations where they believe that data disclosure is necessary to prevent death or serious physical injury. X will honour preservation requests for 90 days, and may, at its discretion, honour requests to extend the preservation period.

The company manages user accounts from two locations. Owing to the GDPR, European accounts are managed from Dublin, Ireland whereas all other personal data is managed from San Francisco, California. Irrespective of location, it requires a search warrant for Direct Messages, Photos, and Tweets. X typically notifies the account holder once their account has been named in a search warrant, however, similar to other platforms, there are exceptions where prohibited by law or where safety is a concern. X also facilitates emergency disclosure requests, which are evaluated on a case-by- case basis and must meet a threshold of "exigent emergency involving a danger of death or serious physical injury to a person."

X's data retention policies reflect GDPR practices. It claims to only hold data from deactivated accounts for a very brief period after which the content is no longer available. Moreover, content removed by an account holder (e.g., a deleted tweet) is not available.

2. *TikTok*[20]

TikTok is a popular social media service focusing on short form video. Messaging between users is a functionality within the service. TikTok originated in China, where it still operates under the

[19] https://transparency.twitter.com/
[20] https://www.tiktok.com/legal/page/global/law-enforcement/en

name Douyin. The non-Chinese version of the service is operated out of Singapore and Los Angeles, California, though the role of the Chinese government remains a matter of considerable debate and has led to bans of the app in some locations. Both the Chinese and non-Chinese versions are currently owned by ByteDance. The Canadian government prohibits use of the service on government-issued devices.

Non-content held by the company data may include:

- Username
- Email address
- Phone number
- Account creation date
- IP address logs
- Video creation time/date

Examples of content data include:

- Video content
- Comments
- Direct messages

Data is encrypted at rest and in transit. The encryption keys are managed by TikTok's U.S.-based security team.

TikTok has three forms of requests: legal requests, emergency requests, and preservation requests**.** All requests from Canadian law enforcement must be made to TikTok PTE Limited, the Singaporean legal entity. The company advises that it may be necessary for law enforcement agencies outside of Singapore to rely on Mutual Legal Assistance Treaties rather than making the request directly to TikTok.

Legal requests require information about the law enforcement agency, the legal basis for the request, and the specific user data requested. Emergency requests can be made in cases of child safety, missing persons, and imminent threats of violence. TikTok's policy is to notify the account holder when their data is disclosed to law enforcement, unless the requesting entity provides a valid reason not to notify the user such as disclosure might hinder investigation or raise safety concerns. TikTok will honour preservation requests for 90 days. It will renew the request for additional 90-day period, but may or may not honour additional extension requests.

The 2022 statistics for Canadian law enforcement requests from TikTok were as follows:

- 57 legal requests were made by Canada in 2022, and 64.9% of those resulted in at least some user data being disclosed to law enforcement
- 184 emergency requests were made by Canada in 2022, and 82% of those resulted in at least some user data being disclosed to law enforcement

- 73 preservation requests were made by Canada in 2022. TikTok's policy is to honour valid preservation requests for 90 days, although TikTok reserves the right not to renew for additional 90 day periods

3. *Snap*[21]

Snap, formerly Snapchat, is a multimedia messaging service that combines photos with messages. Based in California, the service has over 400 million daily active users and 750 million monthly active users worldwide. Snap maintains short retention periods which result in much of their user content being deleted within 24 hour to one month period after either posting or sharing the content. For example, messages are deleted from Snap servers 24 hours after being viewed by the recipient, photos are deleted instantly after being viewed by the recipient.

Since Snapchat is designed to delete images and messages after they are opened, content data which they store is therefore limited to:

- Unopened snaps (images)
- Unopened chats
- Stories (images which stay up for 24 hours)
- Snaps/stories saved by the user

Non-content data held by the company includes user information such as:

- Name
- Username
- Password
- Email address
- Phone number
- Date of birth

Snap considers legal requests for customer data when those requests have a valid legal basis. It considers emergency requests in situations where they believe that data disclosure is necessary to prevent death or serious physical injury. Law enforcement can issue preservation requests which can result in Snap retaining data for a year. The company typically requires use of an MLAT process for non-U.S. requests, though it is known to respond to requests which such process is ongoing, including granting access to basic subscriber information. Snap may, at its discretion, preserve data for up to a year while MLAT processes are being worked on for non-US law enforcement requests. This preservation period can be extended for an additional six months.

From a Canadian perspective, 372 legal requests (involving 617 accounts) were made in the period from January to June 2022. 65.86% of these requests resulted in some data being provided to law enforcement. The company was involved in 2022 case at Quebec Superior Court, which required it to provide the Montreal Police Department with basic subscriber information, transmission data, and location data.[22] The decision in *Re SPVM* concluded that despite the legal

[21] https://values.snap.com/safety/safety-enforcement

[22] Re SPVM (2022 QCCS 3935)

and practical challenges of compelling a corporation to comply with a production order *outside* of Canada, the Court still had jurisdiction to make and enforce the order *within* Canada.

The Court notably concluded that to authorize a production order under the Criminal Code requires only that the company in possession or control of the information be located in Canada or that the person being investigated or the information that is the subject of the production order, and the person in possession or control of the information, have a real and substantial connection to Canada.

iii. Tech Giants

This section reviews the three largest tech giants that also offer messaging or email functionality: Google, Apple, and Microsoft. The primary difference between tech giants and social media services with messaging functionality is the breadth of data collected by the tech giants. Given their exceptionally broad suite of products and services, the companies have access to a wide range of data – notably including financial data – that may be unavailable on other services. Each of the services actively engages with law enforcement on a wide range of requests and policy development. There are some differences with respect to encryption practices, notably Apple's more extensive use of encryption within its consumer products and the limitations on access to encrypted data.

1. Google[23]

Google is the world's largest search engine and owner of a wide range of services including the Gmail email service, YouTube video streaming service, and the Google Play store that provides service to the Android devices. The most common Google products for law enforcement requests are Gmail, Youtube, Google Voice, and Blogger. All of these products contain "content information" such as messages, which are theoretically available to law enforcement if their request is valid. However, the Google transparency report does not provide granular data on which category of data was disclosed.

Content data may involve:

- Email content
- Private messages
- Private videos
- Text messages and voicemail messages
- Private blog posts and comments

Non-content data held by Google includes:

[23] https://support.google.com/transparencyreport/answer/9713961?hl=en#zippy=%2Cwhat-is-a-government-request-for-user-information%2Cwhat-is-an-emergency-disclosure-request%2Cwhat-is-a-preservation-request-and-are-preservation-requests-included-in-the-total-number-of-requests%2Cis-the-data-you-show-in-your-transparency-report-comprehensive%2Cwhy-do-some-of-the-older-reporting-periods-have-less-data-than-newer-reporting-periods

- Subscriber registration information
- Sign-in IP addresses and timestamps
- Upload IP addresses and timestamps
- Billing information

Google's default is that it encrypts data at rest on its servers, and that Google manages the encryption keys. For data in transit, all Google data is encrypted.

Law enforcement requests for data regarding Canadian customers are made to Google LLC, the U.S. entity. The company's position is that requests must be consistent with U.S. law, the law of the requesting country, international norms (specifically the Global Network Initiative's Principles on Freedom of Expression and Privacy), and Google's own policies such as their terms of service, privacy policies, and freedom of expression policies. Google will notify users before data is disclosed, except in limited circumstances such as those involving child safety or if disclosure is prohibited by law. According to its transparency report, 1,164 legal requests were made from January-June 2022, and 82% of those requests resulted in at least some data being disclosed.

Google considers legal requests for customer data when those requests have a valid legal basis. It considers emergency requests in situations where it reasonably believes that it can prevent someone from dying or suffering serious physical harm. Google will preserve customer data while law enforcement applies for the appropriate legal processes to compel disclosure. The preservation request only applies to data which Google holds at the time of the request. The length of Google's data preservation period is not publicly disclosed.

Google requires subpoena for basic subscriber information. A search warrant is required for content information such as messages, documents and photos. Google will notify customers by email before disclosing their information to government authorities, unless doing so is prohibited by law, or if notifying the customer would cause safety issues.

2. *Apple*[24]

Apple is the one of the world's leading technology companies, led by its iPhone, iPad, iWatch, and line of Macintosh personal computer. The company also offers a range of online music, movie, and messaging services. It also maintains a cloud computing backup service (iCloud) that is widely used by consumers. For example, there is an estimated 1.3 billion Messages users.

Given its wide footprint, Apple holds a large amount of customer data, although most of it is non-content data. Some examples of non-content data held by Apple include:

- Basic device registration information (name, address, email, etc.)
- Apple Store transactions
- Mail logs (time and date of emails sent or received, sender and recipient email addresses)

[24] https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

- Connection logs for various products
- Facetime call invitation logs (do not indicate whether a call actually occurred, and do not include any contents of the communications)

Content data is limited to:

- iCloud contents (messages, images, documents, etc.)
- Data extraction from iPhones – only available for some devices running iOS 4 to iOS 7 (iOS 7 came out in 2013)

Apple encrypts some data at the server where it is stored. Other data is end-to-end encrypted. For data that Apple can decrypt, it retains the encryption keys in its U.S. data centres.
Apple does not receive or retain encryption keys for customer's end-to-end encrypted data.

Its transparency reports provide detailed descriptions of what may be made available to law enforcement, subject to appropriate safeguards. Apple considers legal requests for customer data when those requests have a valid legal basis. Emergency requests which relate to imminent threats to physical safety/life, national security, and security of critical infrastructure. Apple will preserve a one-time data pull of the requested customer data for 90 days. This applies to data which Apple holds at the time of the request. Preserved data is automatically removed after 90 days, but the preservation can be extended an additional 90 days upon a renewed request by law enforcement.

Typically, Apple's Canadian corporate entities are responsible for Canadian customer data. Which entity holds the data depends on what Apple product or service is in question. All requests are sent to a centralized email address and triaged by Apple. Apple considers a production order to be a valid legal basis for Canadian law enforcement to request customer data. Requests must be linked to a specific Apple customer using a customer identifier, such as:

- Device identifiers (e.g., serial number or IMEI number)
- Financial identifiers (e.g., credit card or gift card)
- Account identifiers (e.g., Apple ID or email address)

Apple will notify customers unless doing so is prohibited by the court order, or where Apple believes that doing so would create a risk to safety. The company notes that, depending on user settings, some data may be encrypted and inaccessible. Except in emergencies, content data requests must comply with both Canadian law and the U.S. Electronic Communications Privacy Act.

3. Microsoft

Microsoft is the world's most valuable technology company as measured by market capital. The company is best known for its operating system software and suite of computer software and services. However, it is also the owner of a large social media company (LinkedIn), large communications service (Skype), and maintains numerous other online services, including Hotmail, a leading email service, and Microsoft Messenger, a messaging application.

The majority of legal requests relate to Microsoft's free services such as Hotmail. The default for data is that the company holds the encryption keys to customer data, but that customers, particularly large enterprise customers, can hold their own encryption keys. Microsoft's disclosure practices require a court-ordered subpoena for non-content data, while content data requires a warrant. There are exceptions for emergency situations such as violence and self-harm and it may proactively disclose some customer data, for example in instances of suspected child exploitation images.

Examples of basic subscriber information include:

- Email address
- Name
- State, country, zip code
- IP address at registration

Examples of other non-content data:

- IP connection history
- Usernames
- Credit card/billing information

Examples of content data include:

- Email contents
- Files stored on OneDrive or other cloud services

Microsoft encrypts data both at rest and in transit. Many, but not all, products use end-to-end encryption. In most cases, Microsoft stores the encryption keys.

Microsoft considers legal requests for customer data when those requests have a valid legal basis. Microsoft considers emergency requests in situations where they believe that data disclosure is necessary to prevent death or serious physical injury.

Microsoft does not list any public information about preservation requests. Requests must comply with the laws of the requesting jurisdiction. Microsoft challenges requests where the law of the requesting jurisdiction conflicts with the law of the jurisdiction where the data is hosted. Microsoft will notify customers before disclosing their information to government authorities, unless doing so is prohibited by law, or if notifying the customer would cause safety issues.

III. Policy Reform/Key Issues

Lawful access policy has long focused on the role of communications intermediaries such as Internet service providers and wireless providers. However, today's reality is that communications is no longer exclusively mediated primarily through their infrastructure. The

communications layer is obviously essential – network communications naturally requires access to a network – but the information that can be gleaned solely from the network tells only part of the story as billions rely upon social media and messaging applications that pose new access challenges. Indeed, the survey of their policies and practices reveal far wider inconsistencies than those among communications providers that initially prompted the focus on standardized lawful access rules. Indeed, some services retain no data whatsoever, many deploy sophisticated encryption, and some have adopted complex corporate structures with uncertain jurisdictional connections. In fact, even among the best known and well established companies there remains differing transparency and disclosure policies that creates significant challenges for law enforcement operating in time-sensitive situations.

This comprehensive review of current practices and transparency reporting allows for the identification of key concerns for future reforms. Lawful access has long faced a difficult challenge of reconciling law enforcement operational needs with Charter safeguards on privacy and search. These challenges are heightened by social media and messaging apps that are invariably hosted outside of Canada and frequently combine both content and non-content based information. In light of those complexities, this section identifies six key issues that should be the core focus for operational analysis or future policy development.

1. The Challenge Posed By Messaging-Only Apps

The emergence of messaging-only applications such as WhatsApp and Signal have transformed messaging for billions of people worldwide as the services effectively replaced a multi-billion dollar SMS revenue stream for telecommunications companies. The implications for law enforcement is no less transformational. While short messaging was once largely dominated by network providers, the shift to Internet-based services that do not retain nor have access to message content as well as employ strong encryption measures, renders access to such messaging content exceptionally difficult, if not impossible.

Social media services and tech giant messaging remains popular – particularly as an addition to already popular services – and therefore play an important role for investigative purposes. Indeed, the transparency reports from these companies confirms government requests on a near-daily basis. Yet messaging-only services represent a significant hole, providing an easy mechanism to communicate accompanied by significant barriers to third party (or even provider) access. There are no obvious solutions to these technological and jurisdictional hurdles. Moreover, the services play an important role in some societies where the population benefits from the privacy safeguards they provide. The challenge will remain in place for the foreseeable future and will require seeking alternative forms of access and recognition that some providers may be structured in a manner designed to thwart external access to the content of user communications even with appropriate court oversight and privacy safeguards.

2. The Limits of Mandated Data Disclosures

The very concept of mandated disclosure of data stored by social media and messaging apps must be reconsidered. While some services retain data that can be disclosed with appropriate court oversight or administrative safeguards, the reality is that some services retain no data

whatsoever. For example, popular services such as Signal retain little of value to law enforcement, with data limited largely to registration information. This suggests that the provider itself is simply unable to provide authorities with relevant information related to its users. Similarly, "secret chats" on Telegram are not stored by the service, leaving it unable to comply with requests, even if it was willing to disclose. In fact, both Signal and Telegram insist publicly that they have never disclosed content information to third parties. Given the seeming impossibility of legislative intervention to address the issue, certain intermediaries may be technically unable to retrieve information that was previously accessible provided that the appropriate legislative safeguards were met.

Further, even if the company retains some content information, many employ deletion policies that may render the content inaccessible. For example, Snap maintains short retention periods which result in much of their user content being deleted within 24 hour to one month period after either posting or sharing the content. Messages are deleted from Snap servers 24 hours after being viewed by the recipient, photos are deleted instantly after being viewed by the recipient.

3. Jurisdictional Challenges

The jurisdictional challenges posed by the messaging and social media ecosystem represents a massive burden for Canadian law enforcement. The dominance of a handful of Canadian communications providers has raised competition and consumer pricing concerns, but has simplified the situation for law enforcement given the ability to deal with a relatively small number of very large providers. This has had the benefit of fostering personal relationships, developing well-understood policies, and pre-training personnel in advance of time sensitive incidents. Further, Canadian telecommunications laws have largely ensured that providers are Canadian-based and subject to Canadian legislation and the Canadian court system.

The emergence of messaging and social media service represents a near-complete reversal of this dynamic. None of the major services identified in this study are Canadian companies. Further, with the exception of the large global technology companies such as Google, Apple, Microsoft and Meta (the owner of WhatsApp), none even maintain a physical presence in Canada. Indeed, Apple is particularly unusual in that Canadian corporate entities are responsible for Canadian customer data. Canadian jurisdiction rules might still allow a Canadian court to assert jurisdiction if convinced of a real and substantial connection with the country, but enforcement of any court orders (or new legislation) will frequently require mutual legal assistance agreements or additional legal steps in other jurisdictions. This fosters significant uncertainty and delay as part of any process to access information from non-Canadian providers.

Assuming that the jurisdiction issue can be addressed, the applicable law may create another hurdle with some companies painting a confusing picture of mixed requirements. For example, law enforcement requests to Google for data regarding Canadian customers are made to Google LLC, the U.S. entity. The company's position is that requests must be consistent with U.S. law, Canadian law, international norms (specifically the Global Network Initiative's Principles on Freedom of Expression and Privacy, and Google's own policies such as their terms of service, privacy policies, and freedom of expression policies. Apple similarly requires that content data requests comply with both Canadian law and the U.S. Electronic Communications Privacy Act.

While those companies identify the applicable laws, services such as X insist that emergency disclosure requests are evaluated on a case-by-case basis that must meet a threshold of "exigent emergency involving a danger of death or serious physical injury to a person." In other words, the company itself sets the standard for disclosure.

4. Inconsistent Policies

The various messaging and social media services maintain inconsistent rules with respect to their recognized legal approval processes. Indeed, many require court orders from within their own jurisdiction and will not comply when solely presented with a Canadian court order. For example, TikTok requires requests from Canadian law enforcement to be made to its Singaporean legal entity and advises that it may be necessary for law enforcement agencies outside of Singapore to rely on Mutual Legal Assistance Treaties rather than making the request directly to TikTok.

5. Encryption

Encryption unsurprisingly presents another significant challenge. While some services maintain the encryption keys and therefore may be positioned to facilitate access, others simply do not have the technical capability to access user-encrypted content. For example, Microsoft encrypts data both at rest and in transit. Many, but not all, products use end-to-end encryption. In most cases, Microsoft stores the encryption keys. By contrast, WhatsApp cannot and does not produce the content of its user's messages in response to government requests. The content of all messages sent using WhatsApp are protected by an encryption protocol that secures messages before they leaving a user's device, which ensures that only the user and the recipient can listen or read the message. This removes access for intermediaries, including WhatsApp itself. Similarly, Even companies with well-established corporate ownership such as Viber, which is owned by Japan-based Rakuten, have structured their product in a manner in which content data is end-to-end encrypted meaning only the sender and recipient can decrypt it.

6. Uncertainty and Transparency

Despite the existence of transparency reports, there remains considerable uncertainty about social media and messaging services policies on a wide range of issues. This is particularly true for preservation requests. Microsoft does not list any public information about preservation requests, WhatsApp has not disclosed the time period for preservation, and Google's data preservation period is similarly not publicly disclosed.

There are other inconsistencies as between the companies on issues such as the circumstances under which they will disclose requests to affected users. For example, Microsoft will notify customers before disclosing their information to government authorities, unless doing so is prohibited by law, or if notifying the customer would cause safety issues. Viber offers a more robust exception policy, indicating that it notifies users regarding the submission of a law enforcement request prior to the disclosure of any account records, except where: (i) providing notice is prohibited under applicable regulation, court order, subpoena or other legal process; (ii) emergency event occurs and providing a notice could result in a significant risk (e.g., injury or

death) to an individual or a group of individuals; or (iii) an emergency event involves potential harm to minors.

IV. Appendix

See attached