Liability And Disclosure Obligations Of Telegraphic And Electronic Service Providers

Elliott L. Braganza
WeirFoulds LLP, ebraganza@weirfoulds.com
Abstract
Electronic Service Providers (ESPs) are increasingly facing pressures in trial discovery to disclose their clients’ information. But in what situations should ESPs provide this information? To whom do ESPs owe obligations – their customers, litigants or the government? What kinds of information should be disclosed? What standard of proof is required in order to compel disclosure? What kinds of penalties do ESPs risk for failing to disclose information? Judges, litigants, ESPs, and their subscribers have been asking these questions about today’s online world. However, over a hundred years ago, similar questions were asked and answered about the telegraph. By investigating the telegraph caselaw, it may be possible to shed some light on two issues that are of prime concern to an ESP: what are the disclosure obligations of an ESP in litigation? What is the potential liability of an ESP for their part in communicating infringing, libellous and defamatory information?

Keywords
Internet Service Providers, Telegraphs, Disclosure, Liability, Electronic Service Providers

Cover Page Footnote
I wish to thank Profs. Kirsten R. Embree and Monica Y. Song at the University of Ottawa for their feedback in writing this paper.
LIABILITY AND DISCLOSURE OBLIGATIONS OF TELEGRAPHIC AND ELECTRONIC SERVICE PROVIDERS

ELLIOTT BRAGANZA*

INTRODUCTION

Electronic Service Providers (ESPs)1 are increasingly facing pressures to disclose their clients’ information. But in what circumstances should ESPs provide this information? To whom do ESPs owe such obligations—their customers, litigants or the government? What kinds of information should be disclosed? What standard of proof is required to compel disclosure? What kinds of penalties do ESPs risk for failing to disclose information? Judges, litigants, ESPs, and ESP subscribers have asked these questions about today’s online world.2 However, over a hundred years ago, telegraph operators in Canada also had to decide whether to cooperate with disclosure requests or face sanction. In many ways, telegraph operators were in the same position that ESPs find themselves in today.

ESPs face two issues of concern. The first issue is whether an ESP may be liable for its role in communicating infringing, libelous, and defamatory information. The second issue is whether an ESP should comply with a disclosure request and, if so, what kind and how much information they should divulge. This article proposes and concludes that an analysis of telegraph caselaw can assist in shedding light on an ESP’s liability and disclosure obligations.

This article is organized in three parts. Part I begins with a brief overview of the telegraph’s history in Canada, followed by an examination of how Canadian courts have dealt with telegraph operators’ liability and what should be disclosed in litigation. Part II addresses analogous questions for modern Canadian ESPs. Finally, Part III juxtaposes the telegraph and ESP caselaw, identifying the similarities and differences between them. The article concludes with a proposal to advance further work.

* Elliott Braganza was called to the Bar of Ontario in 2013. He completed his articles with WeirFoulds LLP, and holds a Juris Doctor degree from the University of Ottawa. He would like to thank Y. Monica Song in addition to Kristen Embree, for their assistance with this article.
1 Throughout this paper, I use the term Electronic Service Providers to include not only conventional Internet Service Providers (ISPs), but electronic communication systems generally, including, but not limited to, email systems, social networking sites, and corporate intranets.
2 York University v Bell Canada Enterprises (2009), 99 OR (3d) 695 at para 1 [York University].
I. TELEGRAPHS

Telegraphs: History

The first telegraph lines in Canada were constructed in the 1840s, less than a decade after they appeared in Great Britain. The first Canadian lines ran between Toronto and St. Catharines. Eventually, lines connected Toronto with Quebec City and Montreal. Substations were set up in villages located along the lines. By 1847, the Montreal Telegraph Company had constructed 540 miles of wire and had sent 33,000 messages. Like so many other large telegraph companies, the company's charter empowered it to acquire smaller telegraph companies for the purpose of expanding the network.

In the 1850s, the federal government, known then as the Province of Canada, which was responsible for regulating the fast-growing telegraph industry. The “provincial” Act to provide by one General Law for the Incorporation of Electric Telegraph Companies laid out a framework of ownership and organization for telegraph companies. It also granted the companies the authority to erect telegraph lines, and dictated some policy and operational goals. For example, the Incorporation of Electric Telegraph Companies Act specified that messages were to be transmitted in the order they were received, subject to penalties. The government also reserved the right to preferential transmission of messages relating to law enforcement and government business, as well as the authority to retake the lines and nationalize the industry. At Confederation, telegraphs between provinces were specifically excluded from provincial “local works or undertakings.”

Telegraphs: Liability

Telegraph companies faced liability in the same manner as mail or courier delivery services. In delivery disputes, courts relied on the Hadley v Baxendale rule: if a customer made his special circumstances known to the delivery service, and the delivery service breached the contract, the customer would be awarded reasonably

5 Burnet, supra note 3 at 3.
6 Ibid at 5.
7 Ibid.
8 Prov C 1852 (16 Vict), c 10 [Incorporation of Electric Telegraph Companies Act].
9 Ibid at s 10.
10 Ibid at s 12.
11 The British North America Act, SS 1867, c 3 s 92(10)(a).
12 (1854), 9 Exch Rep 341, 156 ER 145.
contemplated damages flowing from the breach. For example, in *Bauld v Smith*, the carrier was held liable for lost profits resulting from a late delivery of a shipment of coal because it was on notice that the coal was required for a cold winter and that market prices fluctuated quickly. Telegraph companies were involved in analogous disputes with their customers, whereby the plaintiff suffered some harm as a result of a miscommunication or a delay by the telegraph company. As a result, telegraph companies developed their own meticulous practices to foster trust in the telegraph service and to avoid insurance claims. For instance, it became common practice to print exclusion of liability clauses on forms given to customers. Telegraph companies were more successful in deflecting legal responsibility as the courts developed doctrines that helped to protect these conduits of information.

In *Stevenson v Montreal Telegraph Company*, the court discussed the liability of a telegraph operator for acts done by an agent in response to the operator’s request but beyond the operator’s control. The defendant telegraph company advertised their services as “connecting with all the principal cities and towns in Canada and the United States.” The plaintiff, in Hamilton, Ontario, had a large quantity of flour under the control of his agent in New York. On Friday afternoon, he instructed the defendant to send a message from Hamilton to the agent in New York to sell the flour. The plaintiff failed to inform the defendant of the importance or time sensitive nature of the message. The telegraph system experienced some problems on Saturday morning, and the Canadian defendant did not send the message until Saturday afternoon. However, the American telegraph operator did not deliver the message to the agent until Monday afternoon, resulting in a loss for the plaintiff by the time the market opened after the weekend.

The court in *Stevenson* began its discussion by holding telegraph operators to a “duty of care and diligence, and with a reasonable degree of skill and efficiency” if they undertook services within their mandate in exchange for consideration. A telegraph operator would be liable for any damages directly and naturally arising from the operator’s negligence and for any matters within the contemplation of the parties when the service was undertaken. The court followed the same approach as *Hadley*. However, the fact that the telegraph operator had advertised service to the United States

---

13. (1901), 40 NSR 294. See also *Cornwall Gravel Ltd v Purolator Courier Ltd* (1978), 83 DLR (3d) 26 (Ont HC) (A modern example, demonstrating the liability of mail delivery service; the defendant courier service was ordered to pay the profit lost by a plaintiff, whose tender was rejected when the defendant, aware that they were delivering the time-sensitive tender, delivered it a few minutes late).

14. Burnet, *supra* note 3 at 126 (“agents were advised to keep accurate records of whom they contacted, arrival and train number, when they notified a customer, conditions of the goods and so on”).

15. (1858), 16 UCQB 530.


18. *Ibid*.
did not mean, in the court’s view, that the operator was warranting responsibility for safe delivery of the message to New York without delay. The American telegraph operator was only an agent of the Canadian operator. The court also found that the contents of the message did not convey a particularly time-sensitive intent.

The defendant telegraph operator transmitted an incorrect message in *Lane v Montreal Telegraph Company*, resulting in liability but not a full award of damages. The plaintiff ship owner had been misinformed by the defendant that he could obtain 8000 bushels of wheat from Chatham when only 3000 bushels were available. Since the plaintiff had given up another contract in order to collect 8000 bushels from Chatham, he sought damages for the lost profits that could have been obtained with 8000 bushels. The court, however, ruled that the plaintiff could only obtain damages for the costs of the voyage to and from Chatham because the intended purpose of the voyage, to sell the wheat for profit, had not been revealed to the telegraph company.

The court in *Kinghorne v Montreal Telegraph Co* denied liability even though the defendant telegraph operator acted negligently. In response to a message from New York requesting delivery of rye for 80 cents a bushel, the plaintiff instructed the defendant to send a message specifying that the plaintiff would deliver “fifteen or twenty hundred.” The telegraph operator’s delivery boy failed to deliver the message to the American representative. The court held that, even if there had been no negligence on the part of the telegraph operator, no valid contract existed due to uncertainty; the message was unclear. The court also held that contracts made by telegraph should observe the same procedures as those made in writing. Arguably, a court attempting to construe a contract would not view the tendency for brevity observed in telegraph messages favourably.

The result in *Baxter v Dominion Telegraph Co* turned on the customer’s familiarity with the defendant telegraph operator’s terms of agreement. The facts of the case are virtually identical to the facts in *Stevenson*. The plaintiffs sued the defendant
telegraph company for failing to deliver a telegraph from Hamilton, Ontario to New York City, resulting in a lost sale to the plaintiff. The court in Baxter held that there was no liability for the defendant telegraph company, and denied the plaintiff’s claim. The court found that since the plaintiff had developed the habit of using a standard form for sending telegraphs, he was deemed to be aware of the conditions that excluded the telegraph company’s liability. The court found that in any case, telegraph operators need a broad exclusion of liability since they face challenging conditions in the course of their duties. The court noted that prudent businessmen might take advantage of the “repeating” function of telegraphs in order to be completely satisfied that messages had been properly delivered.

In Kahn v Great Northwestern Telegraph Co of Canada, a libel case, the plaintiffs attempted to implicate a telegraph company through its role as the conduit of the libelous message. The telegraph company had received some information from a third party regarding the financial standing of the plaintiff. It had then copied the allegedly libellous message into its records, and retransmitted the message to parties. Although the negative portrayal of the plaintiff in the telegram caused the plaintiff damage, the court denied the libel claim. The court cited policy reasons for not wanting telegraph companies to bear liability for libel—companies would have to become arbiters of the contents of the messages that they transmit in order to escape liability.

Telegraphs: Disclosure obligations

In addition to facing personal liability from disgruntled contractors, telegraph companies also had to contend with opening their confidential records up to the inquisitive eyes of litigants. While the Incorporation of Electric Telegraph Companies Act does not make any mention of the record-keeping functions of the companies, the statute made it an offense to disclose the contents of telegraphs:

**Penalty on Operators divulging secrets**

11. Any Operator of Any Telegraph Line, or person by any Telegraph Company, divulging the contents of a private despatch, shall be deemed

---

30 Ibid at para 40 (the court was most concerned with the fragile nature of the telegraph network: “sudden electrical and terrestrial disturbances and accidents, the influence of which may not be felt at the transmitting office, and which cannot be provided against, and over which the company has no control - one can readily see the reasonable necessity of permitting such companies to make contracts and exact conditions limiting their liability particularly stipulating for non-liability as to the working of lines other than their own”) [emphasis added].

31 Ibid. See also Burnet, supra note 3 at 129 (messages were typically sent “unrepeated,” but for an additional fee, usually half the cost of sending a telegraph message, the message could be “repeated” by the sending party, who would confirm the sent message by sending it back to the receiver as transcribed).

32 (1930), 39 OWN 11 (SC H Ct Div).

33 Ibid at para 7.
guilty of a misdemeanor, and on conviction shall be liable to a fine not exceeding twenty-five pounds, or to imprisonment for a period not exceeding three months, or both, in the discretion of the Court before which the conviction shall be had.34

The three-month penalty for breaching confidence was the most severe penalty in the Act. The penalties for other offenses in the Act - wilfully damaging telegraph lines, failing to transmit messages in the order that they were received, and failing to cooperate with Her Majesty during the expropriation of the lines — did not garner the same level of punishment. Telegraph operators took this legislative pronouncement seriously and friction arose when the operators were called on to give evidence in the courts.35

Re New York, Newfoundland and London Telegraph Co36 was one of the first cases to discuss telegram disclosure, albeit within a criminal context. At the time, Newfoundland was not yet a part of Canada, and had enacted its own telegraph statute in advance of the Canadian statute. Section 9 of the Newfoundland statute provided that a telegraph operator would face a penalty if he “wilfully divulged” the contents of a telegraph message.37 In Re New York, a telegraph operator was called by the Attorney General to present evidence before a magistrate of a criminal trial. The operator refused to do so, citing his sworn obligation in the legislation to not disclose telegraph dispatches. The court held that communications in a telegraph office were not privileged communications. Operators who were compelled to attend a judicial proceeding were to disclose these confidences since they were not “wilfully” disclosing them, but rather disclosing them pursuant to the court’s request. The court relied on Lee v Birrell38 for the proposition that those who owe a general duty of confidence must nonetheless disclose to the court upon request.

Leslie v Hervey39 involved the disclosure of telegraphs in a non-criminal setting. The plaintiff sought disclosure from the defendant’s telegraph operator, who refused to do so, citing the section 11 of Incorporation of Electric Telegraph Companies Act prohibition on disclosing private despatches. The court found that no special privilege attached to this type of communication, unlike the privilege associated with the clergy,

34 Incorporation of Electric Telegraph Companies Act, supra note 5 at s 11.
35 Burnet, supra note 3 at 130 (“[a]n established Grand Trunk Railway rule demanded secrecy for all telegrams and their contents by telegraph staff: ‘telegrams addressed to officials must be put in an envelope, sealed and properly addressed in each and every case. The contents of all telegrams must be held as confidential’”).
36 (1861), 4 Nfld LR 575 (SC) [Re New York].
37 Ibid (this section was similar to section 11 of the Incorporation of Electric Telegraph Companies Act, except for the addition of the word “wilfully”).
38 (1813), 3 Camp 337 (UK HL) (case involved the disclosure of property tax books that were subject to a sworn oath of secrecy).
39 (1870), 15 LC Jur 9 (Q Sup Ct).
a spouse, or a solicitor. The purpose of the law was to prevent the unlawful exposure of another’s business or acts and to protect society against “wicked or idle disclosures by telegraph operators.” The right of a litigant to require information relevant to the subject matter of his lawsuit outweighed the right to privacy in telegrams. The court relied on Re New York to justify its position, but did not address the criminal/civil distinction between both cases.

In Baxter, discussed above in reference to liability, the court also discussed the evidence expected of telegraph operators in a civil trial. The court heard evidence that telegraph companies usually keep copies of all messages sent through the lines, and that a telegraph line failure could result in undelivered messages without any notice to the company. The plaintiffs faced a challenge when presenting their case because their chief witness, the telegraph operator who had received the message in New York City, had died by the time of trial. As an alternative, the plaintiffs called those who were acquainted with the deceased. The court stated that, instead, it would have preferred to hear first-hand evidence from the Buffalo telegraph operator who had also handled the message.

A case dating shortly after Confederation highlights the telegraph operator’s dilemma in litigation: should they ignore their responsibility to their customers in favour of their accountability to the public at large? In Re Dwight and Macklam, the court issued a subpoena to a telegraph operator, ordering disclosure of telegrams that had been sent by an election candidate to potential voters. While the company’s policy was to destroy the written telegraph records on a periodic basis, it had not done so when the subpoena was served. Upon receiving the subpoena from the court, the telegraph operator proceeded to burn the written copies of the telegrams in question in delayed compliance with the company policy.

The court held that matters in the public interest militated in favour of disclosure of this information, superseding any private rule that the company may have regarding its records. The court observed that since the subject matter at issue related to elections, a public concern, it could therefore not be privileged. However, the issue of whether the telegraph company could be compelled to disclose information in a dispute between private individuals was left undecided.

40 Ibid at 10.
41 Ibid at 10-11.
42 Baxter, supra note 29 at para 27.
43 Ibid at para 28.
44 (1887), 15 OR 148 (H Ct J) [Dwight].
45 Ibid at para 3 (“[r]ule 83…Each month's messages must be retained for a period of six months after transmission, and then destroyed by fire”) [emphasis added].
46 Ibid at para 10.
47 Ibid at para 16.
48 Ibid.
The court in *Dwight* also discussed whether the owner of the telegraph company or the operator who handled the sending of the telegram should be the proper party to be compelled to appear under a subpoena. The court held that it was simply common sense that if an operator had handled a message, he would be the one to whom the subpoena would be directed since the operator would have ready access to the records. The court specifically noted that parties seeking disclosure of telegrams transmitted by local offices of foreign-owned telegraph companies should not have to direct their inquiries to the foreign offices.

II. ESPS

**ESPs: Introduction**

Tom Standage, in his book *The Victorian Internet*, made the following comment about the telegraph’s relationship with the Internet:

> Although it has now faded from view, the telegraph lives on within the communications technologies that have subsequently been built upon its foundations: the telephone, the fax machine, and, more recently, the Internet. And ironically, it is the Internet—despite being regarded as a quintessentially modern means of communication—that has the most in common with its telegraphic ancestor.

Standage enumerates the similarities between both systems: the ability to communicate over large distances; the belief that the system would solve world problems; the presence of scam artists; the use of encryption and secret codes to prevent unwanted eyes from reading the contents of messages; the initial skepticism but subsequent wide adoption by the business community.

The Federal Networking Council defined the Internet as a global information system that:

1. is logically linked together by a globally unique address space based on the Internet Protocol (IP)...

---

49 Ibid at para 36.
50 Ibid.
51 Tom Standage, *The Victorian Internet* (Markham: Thomas Allen & Son, 1998) at 205.
These layers of the Internet have been described as follows:

**Content Layer**: speech, communications, text, music and video;

**Applications Layer**: email, word processors, Voice-Over Internet Protocol (VoIP) and web browsers are the tools used to transmit the Content Layer;

**Logical / Code Layer**: Transmission Control Protocol/Internet Protocol (TCP/IP), Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) are the conventions used by the Applications Layer to communicate with one another; and

**Physical / Infrastructure Layer**: DSL, cable, satellite, Wi-Fi and fiberoptics provide the physical backbone over which the other layers travel.\(^5^3\)

At the Physical / Infrastructure Layer, the system reduces the complex data for transport into simple bits at the sending end of the system, transmits these bits and reconstitutes the bits in complex form at the receiving end. This paradigm has a parallel to the telegraph, which functioned by first converting the alphanumeric message to Morse Code, transmitting it, and then decoding it on the sending side. But in the case of the Internet, human operators are replaced by electronic routers, which instantaneously translate, transmit and receive an enormous amount of data at a rate far above the telegraph.

This model is able to function efficiently due to the use of IP addresses, which serve to identify and differentiate online parties.\(^5^4\) IP addresses are composed of four numbers separated by periods.\(^5^5\) Once a sending party decides to transmit a stream of data, the stream is parsed into a series of smaller data packets. Each packet contains a header, which is an identifying tag containing both the sending and destination IP addresses. For Internet service subscribers, the ISP is responsible for assigning a

---


\(^5^4\) For the sake of simplicity, only the IPv4 system will be discussed (which is currently in danger of running out of space) instead of the newer IPv6 system.

\(^5^5\) An example would be “255.39.23.9.”
particular IP address to a subscriber. Initially, a subscriber was assigned a static address, but this practice has been displaced in favour of a dynamic address that changes each time the subscriber logs in to the service. Ultimately, it is the ISP that archives which subscriber is assigned to a particular address at a particular time.

**ESPs: Liability**

The question of whether an ESP can be liable for the acts of its users has been codified by Parliament over the last two decades. A starting point is section 2.4(1)(b) of the *Copyright Act*:

2.4 (1) For the purposes of communication to the public by telecommunication …

(B) a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public.\(^56\)

This section was upheld by the Supreme Court of Canada in the case of *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers*.\(^57\) SOCAN challenged a Copyright Board decision that excluded ISPs from liability for copyright infringement occurring on the ISPs’ networks.\(^58\) Initially, SOCAN wanted everyone involved in the conveyance of copyrighted material to pay a royalty, including backbone ESPs who connect the ISPs to the greater Internet, but later limited their claim solely to ISPs.\(^59\) SOCAN also argued that when the ISPs created cache copies in order to increase processing speeds, the defendants became parties to communication and were committing infringement.

The court confirmed that ISPs were merely conduits through which potentially infringing content passed, as per section 2.4(1)(b) of the *Copyright Act*, and could not be held liable.\(^60\) Justice Binnie reasoned that the provision of the *Copyright Act* was not a loophole for ISPs, but an important element of balance struck by the copyright scheme so as to avoid the unfair targeting of the intermediaries involved in telecommunication.\(^61\) He drew upon an analogy to the telephone system, wherein the

---

\(^56\) RSC 1985, c C-42, s 2(4)(1)(b) [*Copyright Act*] [emphasis added].
\(^57\) 2004 SCC 45, [2004] 2 SCR 427 [*SOCAN*].
\(^58\) *Ibid* at para 6.
\(^59\) *Ibid* at paras 14-15.
\(^60\) *Ibid* at paras 92-95.
\(^61\) *Ibid* at para 90.
operators of those systems were not held liable for the messages transmitted through their systems if they were “utterly ignorant” of the message sent. Likewise, only if the ISPs were notified of infringing content on their systems would they be authorizing copyright infringement and potentially liable for that offense. In obiter, Justice Binnie also mentioned that an ESP may perform multiple roles in addition to being an intermediary, and the exemption afforded by section 2.4(1)(b) of the Copyright Act would not apply as a blanket protection if the ESP was actively involved in infringing copyright in another role beyond acting as an intermediary.

The Supreme Court more recently analyzed an ESP’s liability in Crookes v Newton. The court declined to hold a website operator liable for providing a hyperlink to a potentially defamatory webpage. The majority judgment, delivered by Justice Abella, held that hyperlinking did not constitute publication for the purposes of defamation. The hyperlink was merely a reference to another source, and there was a clear distinction between referring to content that was potentially defamatory and actually publishing that content. She rested this conclusion on the fact that the person who inserted the hyperlink in the article had no control over and no knowledge about the content that he or she had linked. This reasoning echoes Justice Binnie’s holding in SOCAN: Internet intermediaries having no knowledge of copyright infringement occurring on their systems should not be held liable.

The recent “Anti-Spam” law contains similar provisions that exempt ESPs from liability:

1. (1) The following definitions apply in this Act. …
   “telecommunications facility” means any facility, apparatus or other thing that is used for telecommunications or for any operation directly connected with telecommunications.
   “telecommunications service” means a service, or a feature of a service, that is provided by means of telecommunications facilities, whether the telecommunications service provider owns, leases or has any other interest in or right respecting the telecommunications facilities and any related equipment used to provide the service.

---

62 Ibid at para 96.
63 Ibid at para 99.
64 Ibid at para 102.
67 Ibid at para 27.
“telecommunications service provider” means a person who, independently or as part of a group or association, provides telecommunications services. …

6. (1) It is prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless
(a) the person to whom the message is sent has consented to receiving it, whether the consent is express or implied; and
(b) the message complies with subsection (2).

…

(7) This section does not apply to a telecommunications service provider merely because the service provider provides a telecommunications service that enables the transmission of the message.68

A similar provision exists in the Copyright Modernization Act,69 which recently amended the Copyright Act. The Copyright Act now provides that a person, in “providing services related to the operation of the Internet or another digital network, provides any means for the telecommunication or the reproduction of a work or other subject-matter through the Internet or that other network” is not liable for copyright infringement.70 Other exemptions are provided for those who operate caching and hosting services.71 In an attempt to keep the legislation attuned to judicial developments, the Copyright Act provides that the exemptions for those who provide hosting services will not apply “if the person providing the digital memory knows of a decision of a court of competent jurisdiction to the effect that the person who has stored the work or other subject-matter in the digital memory infringes copyright.”72 It remains to be seen how these legislative pronouncements will affect the status quo.

---

68 An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23 (the choice of the words “merely because” are important: they insulate an ESP who provides services on the Logical / Code and Physical / Infrastructure layers, who are likely “utterly ignorant” of the content of the messages sent. The wording still allows other types of ESPs to be liable on the SOCAN principle when they engage in non-neutral activities relating to content) [emphasis added].
69 SC 2012, c 20.
70 Copyright Act, supra note 56 at s 31.1(1).
71 Ibid at ss 31.1(2), (4).
72 Ibid at s 31.1(5).
ESP: Disclosure of Identifying Information

Irwin Toy Ltd v Doe\textsuperscript{73} discusses a common issue plaguing plaintiffs who commence Internet defamation or copyright infringement suits: how to identify the “man behind the mask,” the human individual associated with an IP address. With the ability to post anonymously on the Internet, identification of potential defendants becomes a serious issue for plaintiffs. It would be unjust for a plaintiff who has a \textit{bona fide} claim to be unsuccessful but for not knowing the identity of the individual or individuals who wronged them. Similarly, it would also be unjust for a defendant's complete Internet persona to be revealed on the basis of a frivolous statement of claim.

\textit{Irwin Toy} also lays down a general rule indicating when ESPs must identify a subscriber to their service. In this case, the plaintiffs were the subjects of a defamatory email message sent by an ESP subscriber. The plaintiffs requested the identity of the subscriber from the ESP, but the ESP refused to disclose this without a court order. In its judgment, the court began by acknowledging that the ESP was not under any positive duty to disclose the identity of the subscriber. The court found that public policy would be served by maintaining the confidentiality of a subscriber.\textsuperscript{74} The court ruled that a plaintiff is entitled to the disclosure of an ESP subscriber when they demonstrate a \textit{prima facie} case on the merits.\textsuperscript{75} The court saw the \textit{prima facie} case as an effective compromise in balancing the needs of a plaintiff to know the identity of the potential defendant and the potential defendant's privacy.

In the context of a particularly lucrative and contentious issue of copyright infringement, \textit{BMG Canada Inc v John Doe}\textsuperscript{76} relied on the framework set out in \textit{Irwin Toy}. Building on similar American litigation,\textsuperscript{77} a consortium of recording industry players brought a claim against “John Doe, Jane Doe and All those Persons who are Infringing Copyright in the Plaintiffs' Sound Recordings.” The lawsuit named ESPs Shaw Communications Inc., Roger Cable Communications Inc., Bell Canada, Telus Inc. and Videotron Ltee as third parties. The case was first heard at the Federal Court before Justice von Finckenstein.

The unknown defendants in this case were users of the file-sharing programs iMesh and KaZaA, and were subscribers of the named ISPs. The defendants, through the use of their ISP connection and a file-sharing program, were able to search for files located on other users’ systems. Once users found a file that they desired, the program would connect the two users through their IP addresses and transfer the file. The plaintiffs employed a company called MediaSentry and had obtained the iMesh and KaZaA usernames of subscribers who had allegedly shared over 1000 copyrighted

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{73} [2000] 99 ACWS (3d) 399 (Ont Sup Ct J).
\item \textsuperscript{74} \textit{Ibid} at para 11.
\item \textsuperscript{75} \textit{Ibid} at para 18.
\item \textsuperscript{76} 2004 FC 488, [2004] 3 FCR 241 \textit{[BMG Trial]}.
\item \textsuperscript{77} \textit{A&M Records Inc v Napster Inc}, 239 F (3d) 1004 (2001).
\end{itemize}
\end{footnotesize}
songs owned by the plaintiffs. MediaSentry had also obtained what it believed were the IP addresses linked to those users. The plaintiffs sought a court order to compel the ISPs to disclose the identities of these subscribers.

The trial judge began by stating the presumption that the subscribers were entitled to privacy by means of sections 3 and 5 of the Personal Information Protection and Electronic Documents Act. Claims brought frivolously or without any justification were to be avoided, but if a party was involved in the tortious acts of another through no fault of their own and facilitated wrongdoing, they would be under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers. With these concerns in mind, the judge set out a five-part test that would authorize disclosure from the ESP:

(a) the applicant must establish a prima facie case against the unknown alleged wrongdoer;
(b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;
(c) the person from whom discovery is sought must be the only practical source of information available to the applicants;
(d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order in addition to his legal costs;
(e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns.

The court found that the plaintiffs had not met the standard set out in the test. The court was also not satisfied by the evidence linking the usernames from KaZaA and iMesh with the IP addresses provided by MediaSentry.

The Court of Appeal agreed with the trial court's outcome but modified the prima facie test for subscriber identity disclosure set out in Irwin Toy. The court held that requiring the plaintiffs to demonstrate a prima facie case would be too high of a hurdle for them, since identity information is needed in order to make out a prima facie case. Instead, the Court of Appeal ruled that they would only require the plaintiffs to demonstrate a prima facie claim, in that “they really do intend to bring an action for

---

78 SC 2000, c 5.
79 BMG Trial, supra note 76 at para 12.
80 Ibid.
81 Ibid at para 13 [emphasis added].
82 Ibid at para 17.
infringement of copyright\textsuperscript{84} based upon the information they obtain,\textquotedblright; and that there was no other improper purpose for seeking the subscribers\textquotesingle identity.\textsuperscript{85} The court reasoned that the plaintiffs would essentially be stripped of a remedy if they had to make out a \textit{prima facie} case, because they would not have the information to prove the case until examinations for discovery were completed.\textsuperscript{86}

In \textit{York University}, the Ontario Superior Court considered the issue of a \textit{Norwich} order requiring an ESP to produce information before a plaintiff begins a civil action.\textsuperscript{87} An anonymous author had sent defamatory emails and had posted some defamatory material on a website harming the plaintiff. Pursuant to a court order, the plaintiff university had already compelled Google to provide information about a user of a Gmail email address. The plaintiff now sought an order to disclose information from Bell and Rogers; neither ISP opposed the order.\textsuperscript{88}

The court laid out the five-part test from \textit{Norwich Pharmacal Co v Commissioners of Customs & Excise},\textsuperscript{89} which governs when information can be disclosed from a source before an action is started:

\begin{itemize}
  \item [(i)] Whether the applicant has provided evidence sufficient to raise a valid, bona fide or reasonable claim;
  \item [(ii)] Whether the applicant has established a relationship with the third party from whom the information is sought, such that it establishes that the third party is somehow involved in the acts complained of;
  \item [(iii)] Whether the third party is the only practicable source of the information available;
  \item [(iv)] Whether the third party can be indemnified for costs to which the third party may be exposed because of the disclosure . . .; and
  \item [(v)] Whether the interests of justice favour obtaining the disclosure.\textsuperscript{90}
\end{itemize}

Justice Strathy allowed the disclosure, reasoning that the anonymous author could not have sent the emails without the ISPs\textquoteright services. Further, the ISPs\textquoteright privacy policies allowed the disclosure of private communications when service was used for defaming other individuals.\textsuperscript{91} However, the court noted that while Bell and Rogers did not oppose

\textsuperscript{84} \textit{Ibid} at 47 (Court of Appeal disagreed with the trial judge\textquotesingle s characterization of online copyright infringement, and held that the statements were made without a proper hearing of the evidence or a proper consideration of the legal principles surrounding copyright).

\textsuperscript{85} \textit{Ibid} at para 34.

\textsuperscript{86} \textit{Ibid}.

\textsuperscript{87} \textit{York University, supra} note 2 at para 2.

\textsuperscript{88} \textit{Ibid} at paras 3-4.

\textsuperscript{89} [1974] AC 133, [1973] 2 All ER 943 (HL).

\textsuperscript{90} \textit{York University, supra} note 2 at para 13 [emphasis added].

\textsuperscript{91} \textit{Ibid} at para 31.
the application, it would not be in their interests to provide the information without a court order, as doing so may derogate from the contractual relationship with their customers. In cases where the anonymity of the customer was a central issue, the court held that it may be appropriate for the customer to have an opportunity to anonymously present their case.\textsuperscript{92}

In \textit{Morris v Johnson},\textsuperscript{93} the court discussed the issue of anonymous Internet postings and articulated the burden that defamation litigants must meet to obtain a disclosure order. An anonymous Internet poster made comments on a news website article which allegedly defamed the plaintiff, a mayoral candidate. The plaintiff’s Notice of Action requested the site’s moderator, the domain name owner and the operators of the website to assist her in identifying the anonymous poster. The court denied the request because the balancing of interests supported freedom of expression, preservation of privacy, and the vibrant discussion of ideas in an election.\textsuperscript{94} The plaintiff’s statement of claim could have benefited from an elaboration as to which specific words were the source of her harm.\textsuperscript{95} The court employed a modified\textsuperscript{96} version of the \textit{Norwich} order test:

\begin{enumerate}
  \item the third party against whom discovery is sought must be in some way connected to or involved in the misconduct;
  \item the third party must be the only practical source of the information available to the applicant; and
  \item the third party must be reasonably compensated for expenses and legal costs arising out of compliance with the discovery order.\textsuperscript{97}
\end{enumerate}

The court also noted that the plaintiff had not taken reasonable steps to identify the poster through the discovery procedures available in the Rule of Civil Procedure.\textsuperscript{98}

\begin{footnotes}
\item\textsuperscript{92} \textit{Ibid} at para 38. See also \textit{Cohen v Google Inc}, 25 Misc (3d) 945, 887 NYS (2d) 424 (NYSC 2009) (New York Supreme Court allowed a blogger, who used Google’s blogging service, to appear anonymously through counsel in order to defend a defamation claim, instead of Google appearing themselves).
\item\textsuperscript{93} 2011 ONSC 3996, 107 OR (3d) 311 \textit{[Morris]}.
\item\textsuperscript{94} \textit{Ibid} at para 22.
\item\textsuperscript{95} \textit{Ibid} at para 35 (the plaintiff “made reference to the entire posting or article in the Claim and interpreted what the defamatory postings, as a whole, in their natural meaning, and by innuendo meant or were understood to mean” at para 8).
\item\textsuperscript{96} The test was modified to account for the fact that the order was being sought after the action had already begun, as opposed to a traditional \textit{Norwich} order, which is sought before the action is served.
\item\textsuperscript{97} \textit{Morris, supra} note 93 at para 21.
\item\textsuperscript{98} \textit{Ibid} at para 40.
\end{footnotes}
ESP: Disclosure of other types of information

While identifying an anonymous party is one of the most common requests made to an ESP in litigation, the ESP may have other proprietary information that is relevant to the matter at hand. Different considerations emerge in this type of analysis.

The Charter concept of Reasonable Expectation of Privacy (REP) was imported into a discussion of civil litigation in the New Brunswick case of Carter v Connors. In the context of a personal injury insurance claim, the defendant insurer was seeking information about the plaintiff’s Internet usage from the plaintiff’s ISP Aliant. The amount of time the plaintiff spent on Facebook was of particular interest. The defendant believed that the information was relevant because it would show the plaintiff’s capacity for using a computer and accessing the Internet, since the plaintiff was claiming she could not return to her job as an administrative assistant. The court allowed the defendant’s request, since the information had a “semblance of relevance” to the claim. Also, the court found the intrusion was justified because the plaintiff had foregone the normal REP one would have over one’s data by commencing litigation. The quantitative information about the rate of the plaintiff’s Facebook usage would not reveal “intimate details of the plaintiff’s lifestyle and personal choices.” The court ordered that the actual information accessed remain confidential, and that if the investigation required delving deeper into the substance of the plaintiff’s Internet use, the order would have to be re-evaluated.

Although two decisions involving Telus Communications were concerned with Criminal Code provisions regulating when the police can access records for the purposes of investigations, they are noteworthy for their application to civil actions. In the Ontario Superior Court of Justice decision R v Telus Communications Co, the court considered whether information belonging to an ESP could be obtained on a General Warrant, or whether wiretap authorization was required. The police were monitoring two individuals who were Telus subscribers. The Crown requested an order that the defendant ESP would disclose to the police any Short Message Service (SMS) text messages sent between the two subscribers for a specified time in the future.

Siding with the Crown, the court stated that the police should use a General Warrant if they wished to request disclosure of text messages that had yet to be sent.

---

100 Ibid at para 40.
101 Ibid at para 41.
102 Ibid at para 38.
103 Ibid at para 39.
104 RSC 1985, c C-46.
105 2011 ONSC 1143, 105 OR (3d) 411, leave to appeal to SCC granted, [2011] SCCA No 325 [Telus Communications].
106 This type of warrant is available only when no other type of warrant enumerated in the Criminal Code would fit the situation.
between two individuals. Since the police were not requiring real-time wiretap monitoring of these individuals, the court found that it was not an interception of a "private communication" as defined by section 183 of the Criminal Code.\(^{107}\) Telus argued that the Crown should seek a warrant at the end of each day requesting the SMS messages sent for that day. The court saw this as impractical and decided that the General Warrant was the proper mechanism to use when seeking prospective disclosure.\(^{108}\) The reasons cited by the court for the impracticality of Telus’ suggestion were:

a) fourteen applications as opposed to one application;

b) the probable need for the involvement of more than one Justice of the Peace;

c) the possibility of inconsistent approaches by different Justices of the Peace; and

d) inconvenience to the person to whom the warrant is directed, in receiving a daily warrant requiring prompt response.\(^{109}\)

The court limited the ambit of the Warrant to only capture messages sent after the date the Warrant was issued, and struck down the part of the Warrant that sought disclosure of messages sent before the date of the Warrant.\(^{110}\) The court found that these requests should instead be brought under the framework set out in sections 183, 185, and 186 of the Criminal Code. While the court found that these messages were more akin to business records than communications, it noted that Parliament was in a better position to decide if a text message should be deemed a communication rather than a record.\(^{111}\)

Tele-Mobile Co v Ontario\(^{112}\) considered whether an ESP or the state should bear the costs of complying with Criminal Code “production orders”. Pursuant to section 487.012 of the Criminal Code, these orders are obtained by police against third parties who have access to documents and data relevant to criminal investigations. The Toronto Police Service and the Ontario Provincial Police had obtained production orders, seeking information relating to murder and drug investigations. The orders required Telus to expend considerable financial resources to obtain the information. The court pointed out that the Criminal Code did not contain any provisions directly relating to ESP compensation for these types of undertakings. There was only a general provision allowing a judge to make an order that could specify “any terms and conditions that the

---

\(^{107}\) Telus Communication, supra note 105 at para 49.

\(^{108}\) Ibid at para 76.

\(^{109}\) Ibid at para 70.

\(^{110}\) Ibid at para 89.

\(^{111}\) Ibid at para 61.

\(^{112}\) 2008 SCC 12, [2008] 1 SCR 305 [Tele-Mobile].
justice or judge considers advisable in the circumstances.”  Telus unsuccessfully argued that this general provision provided authority for allowing reasonable compensation from the state for compliance. The court interpreted the legislative silence on compensation as supporting the proposition that a general “moral” and “social” duty imposed on citizens requires them to comply with these sorts of orders without compensation. The court only allowed compensation where compliance with the order would result in unreasonable expense.

III. JUXTAPOSING TELEGRAPH AND ESP CASELAW

There are several parallels drawn between telegraph cases and their Internet counterparts. The similarities between the two sets of jurisprudence arise from the analogous ways in which the systems operate. Both a telegraph customer and an Internet customer provide information to the provider to be transmitted with the understanding that it will be delivered by the ESP, subject to the terms of the agreement. Under both systems, the content and destination of the information are archived by the service provider, either by paper for telegrams, or electronically by an ESP. Both systems may encounter a situation where the information must be sent to a destination that is outside of the service provider’s network and where an agent of the ESP must subsequently complete the delivery of the information. It should also be noted that the construction of telegraph lines and the modern telecommunication infrastructure were partially funded by public money.

However, there are important differences to keep in mind when attempting to draw comparisons between these two series of cases. While the telegraph and the Internet both function by transmitting “dumb code,” the Internet handles a much greater load of information than the telegraph ever could. As a result, Internet operators are not in a position to scrutinize all the data passing through its system unlike a telegraph, which relies upon human operators transcribing the information for transmission. Also, there is a greater likelihood that information sent through the Internet would be accessible to a broader audience due to the relative ease of sharing information online. Torts committed online, such as libel and defamation, have the potential to unleash greater harm than a single libelous or defamatory telegram. Finally, Internet communication has the capability of involving multiple service providers simultaneously, such as using an ISP to access a social networking website to share an online video. In such a situation, the ISP, the social networking site and the online video

113 Ibid at paras 41, 44.
114 Ibid at para 50.
115 Ibid at para 52 (the court noted that annual costs of Telus’ compliance with the order were on the order of $662,000.00, but that this constituted only a small fraction of Telus’ annual revenues and operating expenses at para 68).
provider would all be potential ESPs. This does not have an analogue in the telegraph industry.

1. ESPs’ duty to assist private litigants

Perhaps the most pressing question for ESPs in non-Criminal Code situations would be determining when an ESP must supply information on request. While a service provider may decide to provide information to the police on the basis of helping to solve and prevent crime, the service provider cannot use the same rationale when dealing with a dispute between two private parties. For example, the telegraph operator may owe a confidentiality obligation towards their customer as a result of a contract or, as in much of the caselaw, a statutory bar which prevents disclosure of the contents of telegrams. A modern ESP may choose as a matter of principle to maintain their paying customers’ privacy.

The answer to this question is that there is a duty upon ESPs to assist litigants if they have a bona fide claim, but the litigant must first obtain a court order. This issue was confronted in parallel cases, separated by 139 years: Leslie (1870) involving the telegraph, and York University (2009) involving the Internet. In both cases, the court had to determine the standard a litigant must satisfy in order for there to be sufficient grounds to compel the disclosure of information. In Leslie, the court permitted disclosure, rationalizing that the guarantee of privacy in one’s affairs cannot extend past the rights of a litigant who has a suit pending. Disclosure would be granted if it brings facts bearing on the subject matter of the suit to light. In York University, the test became more stringent, although similar reasoning was used—privacy cannot be preserved absolutely and, if a litigant cannot obtain the information by other means, the ESP must disclose it. Instead of requiring that the information be provided simply if it exists in the ESP’s archives, the information must only be accessible this way.116

2. ESPs must abide by public service obligations

As mentioned above, both the telegraph lines and the Internet substructure were constructed at least partially with public funds. Therefore, it is no surprise that providers are expected to comply with the government’s request for information for its own purposes. The 1851 telegraph legislation provided for preferential transmission of government information and the possibility of industry nationalization, both of which allowed the government to exert considerable control over the network’s functionality. In Tele-Mobile, Justice Abella stated that disclosure requests from the government are

116 York University, supra note 2 at para 27.
“neither unanticipated nor aberrational,” but rather reasonably incident to an institution’s operation.\textsuperscript{117}

The courts also encouraged disclosure by telegraph operators when the public interest demanded it. Recall \textit{Dwight}, where the court placed a higher value on the public interest in investigating electoral fraud than the telegraph company’s policy of destroying sent telegrams. \textit{Re Huston}\textsuperscript{118} came to a similar conclusion 35 years later. In that case, a Commissioner conducting an investigation under the \textit{Public Inquires Act}\textsuperscript{119} required a telegraph operator to reveal information the Commissioner determined necessary for a “full investigation of the matters into which he is appointed to examine.”\textsuperscript{120} This was the case notwithstanding the statutory declaration that telegraph operators were to hold information in confidence.

\textit{Telus Communications}, discussed above, unfolded under a considerably more complicated regime, but the intent in that case was the same as \textit{Dwight} and \textit{Huston}. Once again, a service provider was called upon to provide information to aid in the public policy objective of crime prevention, and the court ruled in favour of this objective.\textsuperscript{121} There is a common thread in these cases: courts gave the government authorities the benefit of the doubt when the investigation was conducted in the public interest. Therefore, it is possible that investigative bodies, like the Competition Bureau, may also be able to rely on public policy to justify disclosure. However, these requests will likely be under greater court scrutiny because investigative bodies would also be subject to the \textit{Charter} unreasonable search restrictions and would have a narrower ambit of discretion granted to them than peace officers. As a result, it is unlikely that private parties seeking disclosure from ESPs would be able to rely on public policy objectives to justify disclosure.

3. Unwillingness to blame the ESP

The courts are reluctant to penalize communication service providers for providing means by which infringing information may be communicated.\textsuperscript{122} In \textit{Kahn}, the court emphasized that telegraph operators were not to become arbiters of content and absolved the telegraph company from liability in that case. The telegraph operator in \textit{Stevenson} also benefited from the court’s strict interpretation of the agreement between the customer and the operator—advertising telegraph service to New York

\begin{itemize}
  \item \textsuperscript{117} \textit{Tele-Mobile}, supra note 112 at para 60.
  \item \textsuperscript{118} (1922) 52 OLR 444 (Ont Sup Ct (AD)) \textit{[Re Huston]}.
  \item \textsuperscript{119} SO 2009, c 33, Sched 6.
  \item \textsuperscript{120} \textit{Re Huston}, supra note 118 at para 26.
  \item \textsuperscript{121} However, the issue here is not whether the service provider must disclose information or not, but whether the service provider can be bound to provide the information in the future.
  \item \textsuperscript{122} The term “infringing information” here refers not only to copyright infringement, but also more generally to any type of legally actionable wrong, such as defamation and libel.
\end{itemize}
from Canada did not amount to advertising safe transmission of a message to New York without delay. Similarly, in *BMG Canada v Doe*, the ultimate defendants in that case were the John Doe file sharers rather than the ESPs.\(^ {123} \)

Recall the legislative enactments which now provide a level of protection for certain types of ESPs, and how the provision in the *Copyright Act* was tested in *SOCAN*. The reasoning in *SOCAN* closely echoes what was said in *Kahn*, even if the remedies sought were different: *SOCAN* was seeking royalties for copyright infringement, while *Kahn* was seeking liability for defamation. In both cases, the courts held that service providers, whose business it is to coordinate communication between a large number of parties, should not be held liable unless the service provider inspects and sanctions the contents of infringing communications. This is echoed in the modern *Copyright Act*, which states that a factor in considering whether an ESP has infringed copyright is whether they “had knowledge that the service was used to enable a significant number of acts of copyright infringement.”\(^ {124} \) A rationale for this may be found in the *Kinghorne* decision. Even though the harm may not have occurred but for the service provider’s involvement, the service provider handles so many communications that they cannot bear the burden for every party that communicates. The compensation for providing this service would be considerably smaller than the potential harm.\(^ {125} \)

**4. Who bears the cost of compliance with ESP disclosure orders?**

The modern costs of compliance with ESP disclosure orders are substantial. In *Tele-Mobile Co v Ontario*, Telus estimated their annual costs for compliance with these orders to be roughly $662,000.00, more than “a mere bagatelle.”\(^ {126} \) The costs run high because retrieving information from voluminous ESP archives is time consuming and labour intensive.\(^ {127} \) Who should carry the costs of these requests?

The answer echoes what was said above in reference to disclosure: ESPs will be expected to provide their services gratuitously when the public interest demands it, while private parties will be expected to bear their own burdens. In criminal matters such as *Tele-Mobile*, the court ruled that the ESP would be responsible for all reasonable costs, since compliance with these orders fits the principle of the citizenry

---

\(^{123}\) It must be noted that the ESPs were the immediate subject of the motion brought by the recording industry plaintiffs.

\(^{124}\) *Copyright Act*, *supra* note 56 at s 27(2.4)(b).

\(^{125}\) *Kinghorne*, *supra* note 24 at para 49.

\(^{126}\) *Tele-Mobile*, *supra* note 112 at paras 68-69.

\(^{127}\) *ibid* at para 8 (“[T]he process for the recovery of archived data includes identifying and locating the relevant magnetic tapes, arranging for their transport from an off site location back to our computer processing facilities, mounting the tapes onto a dedicated storage facility, searching the tapes and processing the search results. There are substantial labour and equipment costs engaged by this process”).
aiding in the efficient administration of justice. In *York University*, Justice Strathy allowed the order on the basis that the plaintiff would remunerate the ESPs conducting the search for the plaintiff. The forth branch of the *Norwich* order test requires that “the third party be indemnified for costs to which the third party may be exposed because of the disclosure,” which includes the costs of complying with disclosure.\(^\text{128}\)

The telegraph cases make no mention of the actual costs of compliance, possibly because the amounts were negligible. However, the courts in these cases did discuss penalties for failing to comply with the court’s orders. In *Re New York*, the lower court was prepared to find the telegraph operator in contempt for adhering to the oath of secrecy.\(^\text{129}\) In *Dwight*, the court fined the telegraph operator $100.00 for destroying the telegrams in question.\(^\text{130}\) The court decided not to imprison the operator and reduced the fine due to a finding of fact that the operator was following the orders of a superior.\(^\text{131}\)

**CONCLUSION**

Those analyzing the Internet from a legal and policy perspective could benefit from looking to the law of the telegraph. While not directly analogous to the Internet, this body of law provides, at the very least, a starting point for discussion in an area that seems to lack precedent. Certain areas show close similarity: the standard for both electronic and telegraphic disclosure in non-criminal cases requires proof of a *prima facie* claim. In cases where the public interest was engaged, both telegraph operators and ESPs were expected to disclose information on request by government. Still, there are important differences. Telegraph service providers faced a greater likelihood of legal liability compared to their electronic counterparts in the online world. Statute and the common law have stepped in to provide broad legal protection for these modern service providers as recognition of their part in facilitating communication. However, in exchange for the privilege of offering their services, modern ESPs must bear financial liability for subsidizing government requests for information. Even with these differences, the law of the telegraph should not be forgotten when novel questions about the Internet or its successors arise.

---

\(^{128}\) *York University*, *supra* note 2 at paras 13, 28.

\(^{129}\) *Re New York*, *supra* note 36 at 575.

\(^{130}\) *Dwight*, *supra* note 44 at para 41.

\(^{131}\) *Ibid* at para 40.