

## INFORMATION ETHICS IN THE ELECTRONIC AGE:

CHAPTER 20: THE ROLE OF ISPS IN THE  
INVESTIGATION OF CYBERCRIME

IAN KERR AND DAPHNE GILBERT

In July of 1993, a now famous cartoon was published in the *New Yorker* magazine).<sup>1</sup> The cartoon depicts a large black pooch with big floppy ears, sitting on an office chair in front of what is by today's standards a rather clunky PC. The pooch—who is talking to a smaller and extremely attentive pup—remarks that, "On the Internet nobody knows you're a dog." Besides being humorous, the cartoon demonstrates an important cultural discovery— in 1993, converging communications technologies created the possibility of online anonymity.

In fact, back in 1993, relative anonymity was a central feature of Internet communications. Not unlike the citizens' band radio, it allowed for a kind of open and unfettered conversation not typically experienced in public spaces. AIDS victims and child abuse survivors found, for the first time, a safe place to congregate, emote and share vital information.<sup>2</sup> Because the Internet allowed for communication that was not self-authenticating, it promised to those interested in exploring personal identity and the social construction of personality a pro-found kind of plasticity. As Lessig describes it, "Here the ugly can speak seductively, or the shy can speak — period."<sup>3</sup>

There is a less famous but perhaps more telling cartoon that appeared in April 2000, riffing on the observation made by those two dogs seven years earlier. In the latter cartoon, one dog opines to the other that "The BEST thing about the Internet is THEY don't know you're a dog." But, as those words were barked, a voice from within the computer responded to the talking dog, "You're a four-year-old, German Shepard-Schnauzer mix, likes to shop for rawhide chews, 213 visits to Lassie Web site, chat room conversation 8.29.99 said third lassie on the right was hottest, downloaded 3rd Lassie 10.12.99, E-mailed them to 5 other dogs whose identities are...."<sup>4</sup>

This response signifies an important shift not only in the culture of the Internet but also in its architectures. As the second cartoon illustrates, there is often a commercial interest in knowing who is doing what online. In furtherance of this interest, persistent client state http cookies, keystroke monitoring and a number of other surveillance technologies have been developed to gather data and otherwise track the movements of potential online customers.<sup>5</sup> Such curiosity, however, is not unique to business. Concerned that computer networks and electronic information may also be used for committing criminal offenses (and

knowing that evidence relating to such offenses may be stored and transferred through these networks), many countries are considering the adoption of legislation that would require service providers to build a communications infrastructure which would allow law enforcement agencies to gain access to the entirety of a specific telecommunication transmitted over their facilities.<sup>6</sup>

In this chapter, we argue that the legislative approach that is about to be adopted in various jurisdictions around the world is highly problematic, as it will lower the threshold of privacy protection and will drastically alter the relationship between Internet service providers (ISPs) and the individuals who have come to depend on them to properly manage their personal information and private communications. We begin with a brief investigation of the role of ISPs as information intermediaries. We then examine a recent case<sup>7</sup> which held that an ISP acted as an "agent of the state" when it voluntarily assisted the police in an investigation by disclosing a customer's personal information and private communications. The "agent of the state" concept and the changing nature of the relationship between ISPs and the state are further explored through an articulation of various kinds of investigatory information that can be collected by ISPs on behalf of the police, followed by a discussion of the call for a lower threshold for obtaining such information in the European Convention on Cybercrime.<sup>8</sup> We conclude by arguing that the shifting architecture of our communications infrastructure must be built with various safeguards that will not only further the goals of national security and law enforcement but will also preserve and promote personal privacy.

## DISINTERMEDIATION

For nearly a decade, scholars have focused their attention on the Internet as an instrument of disintermediation. Recognizing that intermediaries are valuable to a transaction only if they are as inexpensive as equivalent functions found in an open market, many scholars have in fact predicted that the Internet—which reduces transaction costs by allowing direct interaction between manufacturers and consumers — will have the effect of "killing the man in the middle."<sup>9</sup> Consider the following typical statement:

Unlike tomatoes or cars, real estate listings, stock quotations, and airline schedules are bits, easily and inexpensively shipped at the speed of light. Bits need no warehousing, and the cost to make more is effectively zero. For this reason, real estate agents, stockbrokers, and travel agents will disappear much more rapidly than food wholesalers or car dealers.<sup>10</sup>

While it is perhaps true that the disintermediation phenomenon occurs in the context of some business transactions, disintermediation is clearly not a universal by-product of Internet communications. In fact, online intermediaries remain quite relevant to other aspects of almost every Internet communication. ISPs are the Internet's "middlemen." Because ISPs are the pipeline through which all of our online communications must flow, they are in a position of control. More and more, ISPs are in a position to observe and record everything that we say and do online. Thus we are increasingly forced to rely on ISPs, not only to provide quality informational services but also to store and otherwise manage our private information. Consequently, we have come to depend on them to safeguard our personal information and private communications and to prevent that information from falling into the hands of third parties.<sup>11</sup> This gives ISPs power and discretion: power

to control our online behavior and discretion to alter our outcomes.<sup>12</sup>

The shifting architectures of the net-worked world currently allow ISPs automatic access to their customers' and employees' personal information and private communications in a manner unparalleled by even the most powerful financial institutions or arms of government. As is further discussed below, one of the central strategies of the Convention on Cybercrime (and corresponding legislation likely to be enacted in various jurisdictions around the world) is to mandate a communications infrastructure that would allow law enforcement agencies to capitalize on the informational power held by ISPs. In this respect, ISPs already play and will continue to play an absolutely critical role as information intermediaries. They are the stewards of our personal information and private communications. This fact is well illustrated by a well-known case in Canada — *R. v. Weir*.<sup>13</sup>

### R. v. WEIR

Having inadvertently exceeded his available disk quota, Mr. Weir was having trouble one day accessing his email. Trusting his ISP to fix the problem on his behalf, he called the next morning to request the assistance of a technician and then went off to work. While Weir was at work, the technician discovered the problem. Mr. Weir had too many emails with large attachments residing on the host server. The excessive size of these files automatically disabled his account. The technician approached the problem in the standard way. Files were opened so that the attachments could be moved off the server. In so doing, the technician discovered that the names of certain files sent to him that day sounded suspiciously like titles typical of child pornography. The technician informed his manager of his discovery, and the manager, in turn, decided to alert the Edmonton police. The police insisted that the ISP was to forward copies of the files. It further instructed the ISP to re-enable Mr. Weir's account so that the files that he had been sent (but had not yet received) would come to be in his possession.<sup>14</sup> Weir's ISP capitulated.

The facts in the Weir case are illustrative of the role that ISPs are being asked to play in law enforcement with increasing frequency. On the basis of the transactions that took place between his ISP and the police, a search warrant was obtained, and Mr. Weir's computer was seized.<sup>15</sup> What is so telling about this case is that it was initiated entirely at the discretion of the ISP. Because it was the pipeline through which all of his private communications must flow, Weir's ISP was in a position to know the content of his and the senders' online communications and was in a position to choose whether to contact the police or let them go about their private business. The important point to be gleaned from this case is that, in the context of investigatory information, the architecture of the Internet does not disintermediate. Rather, it has quite the opposite effect. It requires an ISP to intermediate between two potentially conflicting roles: (1) its role as the trusted steward of its clients' personal information and private communications; (2) its role as a party in possession of information that might assist in law enforcement.

At trial, Mr. Weir's defense counsel argued that Weir had a reasonable expectation of privacy in his email, as well as a constitutional right to be secure against unreasonable search and seizure. He argued that the manner in which the police used the ISP to obtain evidence against his client was unconstitutional. The trial court was not persuaded. Although the court agreed that the police were prohibited by the constitution from conducting an unauthorized search, it held that the usual constitutional safeguards simply do not apply to searches

conducted by a private sector service provider. According to Justice Smith:

[I]t cannot be said that the ISP was performing a governmental function. ISPs are private organizations. They are unregulated... With international agreements, it may come to pass some time in the future that ISPs will be regulated.... [T]he wish found in Canadian Government documents for such regulation is no more than a "pious hope" today.<sup>16</sup>

Weir appealed this decision, arguing that the trial court erred in its finding that the ISP was not performing a governmental function. Relying on a doctrine in criminal law known as the "Broyles Test,"<sup>17</sup> Weir argued that his ISP was acting as an "agent of the state."

## ISPS AS AGENTS OF THE STATE

The agent-of-the-state argument usually arises in the context of an investigation carried out by a private citizen. The most typical instance occurs when police send an informant rigged with a body pack into a holding cell with the aim of intercepting and recording a confession that is teased out of an accused person. Where the accused has already invoked the right to silence and remains in the coercive environment of a jail cell, the agent-of-the-state doctrine prohibits the police from doing indirectly that which they cannot directly do. In such instances, the court considers the collection of the evidence to be unconstitutional in spite of the fact that it was obtained not by the police but by a private citizen. Although private citizens are not generally bound by the same constitutional duties that bind the police, where the informant is carrying out a police-type function, they are considered agents of the state, and the evidence is therefore inadmissible. The test for whether a private informer is acting as an agent of the state is as follows:

[W]ould the exchange between the accused and the informer have taken place, in the form and manner in which it did take place, but for the intervention of the state or its agents?<sup>18</sup>

Applying this test to the facts in the Weir case, the Court of Appeal held that the ISP was acting as an agent of the state when it forwarded, at the request of the police officer, a copy of the messages sent to Mr. Weir. On the basis of this finding, the Court of Appeal held that the police's subsequent search of Weir's home was unwarranted.

It is our contention that the application of the agent of the state doctrine to ISPs is extremely significant. By treating ISPs who cooperate with law enforcement as state agents, the courts have recognized the shifting role of ISPs. ISPs and other information intermediaries are no longer in a position to promise absolute confidentiality to their clients or to act as the guardians of their informational privacy. Nor are ISPs merely the conduit through which their clients' personal information and private communications flow. Rather, ISPs are now seen as a reservoir of personal information and private communications — a reservoir that can and will be tapped by the state for the purposes of law enforcement.

It is our position that this very recent shift in the nature of the relationship between ISPs and the state must be recognized, as it will clearly alter the manner in which investigatory information is collected in the context of criminal law. These alterations will in turn affect personal privacy. We turn now to a brief examination of the kinds of information that can be collected by ISPs on behalf of law enforcement and the call for lower standards of accountability in the collection of such information pursuant to the Convention on Cybercrime.

## INVESTIGATORY INFORMATION

In the course of sending an email or surfing on the Web, Internet users produce an array of information that is potentially relevant to a criminal offense investigation. The European Convention on Cybercrime loosely describes three types of information in its various articles. The domestic legislative proposal in Canada to ratify the convention adopts a more formal approach to definition but maintains these three categories: customer name and address and local service provider identification ("CNA/LSPID"); traffic data; and content data.<sup>19</sup> These categories are significant because they define the increasing level of privacy expectation that attaches as one moves from CNA/LSPID through to content. A user's expectation of privacy in the information is crucial to whether a search and seizure of that information requires judicial preauthorization (through a warrant or intercept order) and is thus constitutionally protected. These three categories are controversial in definition because it is by no means intuitive what kinds of information necessarily falls into each category.

CNA/LSPID is commonly conceived of as the "lowest" level of investigatory information, with the lowest expectation of privacy. An online service, such as Yahoo! mail, could be required by law to divulge the local service provider identification of an email user. The local service provider would then be asked to identify the name, address and billing information of its client. This information carries the lowest expectation of privacy as it is likened to information that is available in a telephone directory.

The second, or "medium," level of investigatory information sought by law enforcement is traffic data. The Convention on Cybercrime defines traffic data as:

any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.<sup>20</sup>

Conceivably, traffic data would include the information carried in the sender, recipient and subject lines of an email and its size (which would in turn reveal whether there are attachments to the email). It could also include the titles of attachments (which might then indicate by the extension whether the files were photographs or video clips), and the websites visited by a user and the time spent at each. Traffic data make up a roadmap of a user's Internet communications as one travels along the information superhighway.

The third, or "highest," level of investigatory information is content data. This category would include the text of email messages. It might also include the search terms entered into an Internet search engine. It is our position that the line between traffic and content data is tenuous and that it is difficult to demarcate what constitutes "content." This ambiguity gives rise to two problems. First, information collected and stored for one purpose can be combined with information collected and stored for a completely different purpose through data mining.<sup>21</sup> Two pieces of seemingly innocuous information might prove damning in the combination — an effect which is illegitimate in its failure to respect the original purpose behind the collection of each piece of data. The conclusions possible through data mining might also reveal something more akin to what a user considers "content." Second, the information revealed by the roadmap of traffic data could itself be considered content. Queries to an Internet search engine are a good example. While some might describe search terms as steps toward accessing Internet content, it is worth noting that these queries could well be indicative of the content of a user's time

surfing on the Internet, similar to the content of an email. Similarly, it might be said that the size of an email and the names and extensions of attachments, especially when combined with other data, provide information that is just as revealing as content data.

These three categories compose the various types of information sought by law enforcement during the course of a typical investigation. While it may be a useful heuristic device to treat these categories as distinct, one must recognize the social implications of distinguishing these categories in this way. Our concern is that an oversimplification of these categories could have an effect on the overall attitude toward Internet privacy adopted in the convention and domestic laws in Canada and the United States. The working assumption seems to be that only content is or should be protected by the higher standard of judicial preauthorization. Impliedly, Internet users have little or no expectation of privacy in either their name, address, or more significantly, the list of emails sent and received or websites visited. This approach also has the detrimental effect of placing an enormous demand on ISPs. It requires ISPs to distinguish between traffic and content data and to assist in the data-mining process by complying with judicially authorized searches. It also requires ISPs to build and maintain an infrastructure specifically designed to assist law enforcement, in the form of a global intercept capability. This new role is mandated by the convention in the context of a general international treaty that leaves much to the discretion of participating states in actual implementation.

## CONVENTION ON CYBERCRIME

On November 23, 2001, the members of the European Union and several non-member States signed the convention.<sup>22</sup> It emphasizes the concern that computers are used to commit criminal offenses and the fact that information stored or transmitted through computer systems might be evidence of a crime.<sup>23</sup> It stresses the need for international cooperation in the detection, investigation and prosecution of criminal offenses and the corresponding need for investigatory powers.<sup>24</sup> The convention recognizes "the need for co-operation between States and private industry in combating cyber crime and the need to protect legitimate interests in the use and development of information technologies."<sup>25</sup> Importantly, it also emphasizes human rights, including rights to freedom of expression and privacy, and it recognizes the need to protect personal data.<sup>26</sup> The convention's text demands two broad requirements: measures at a national level to implement the convention's terms and international cooperation to investigate criminal offenses.

In Chapter 11 ("Measures to Be Taken at the National Level") the convention divides its requirements into substantive and procedural criminal law. The substantive criminal law section asks signatories to create several offenses, including unlawful interception, access or interference with a computer system, computer-related forgery and fraud, and offenses relating to child pornography and copyright. The procedural law section is our focus. It outlines sweeping new investigatory powers for law enforcement and mandates access to all information stored and transmitted on computer systems. Access to this information will be facilitated by ISPs.

Three types of judicial orders are considered in the convention: (1) preservation, (2) production and (3) interception. Each has disturbing ramifications for privacy interests. Despite its articulation of a concern for privacy and data protection, the convention makes no further reference to balancing these concerns against the new investigatory powers accorded to law en-

forcement. The convention is silent as to the judicial preauthorization standard for each order contemplated. There are some hints, however, to the nature of each order envisioned and the corresponding level of privacy intrusion.

The convention outlines two types of preservation orders. The first consists of expedited orders to preserve specified computer data, including traffic data, stored on a computer system.<sup>27</sup> The convention suggests that the initial expedited order extend to a maximum of ninety days while the authorities seek disclosure of the information. A two-pronged approach is envisioned. Presumably, it should be easier for authorities to get the initial, expedited preservation order, especially since the article stresses that it is targeted at data that is "particularly vulnerable to loss or modification."<sup>28</sup>

The second order for disclosure of the information could be more involved. The wording of this article is confusing in its separation of specified computer data from the direct reference to "traffic data." It appears therefore that the ISP would be asked to preserve all data, including content, for up to ninety days (provision for a renewal of the order is optional). The consequences of such an order are staggering and form the basis for our assertion that the convention fundamentally shifts the role of ISP from that of a conduit to a reservoir of information. For a period of up to three months, every piece of information a user inputs into the Internet, through email or Web use, could be preserved by the ISP for access by law enforcement.

The convention outlines a second preservation order (and partial disclosure order) for traffic data.<sup>29</sup> It is clear that this order should be granted on a low standard of justification, for it is designed to be expeditious. While Article 17 refers to "traffic data," it is actually targeted at the lower-level CNA/LSPID information, for it mandates disclosure of "a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted."<sup>30</sup>

The second broad type of order contemplated by the convention is a production order. This order is also broken down into two types: a general production order, directed at a person for "specified computer data," and an order against a service provider for "subscriber information."<sup>31</sup> While the convention is silent as to its reasons for the division, it must be assumed that by distinguishing the orders, the drafters envisioned different standards for each. Presumably, the order against an ISP for subscriber information would require a low level of justification. This would be consistent with the privacy interests typically accorded identify, address and billing information.

Finally, and perhaps most dramatically, the convention mandates real-time collection or interception of both traffic and content data. It provides that state parties should compel ISPs to collect and record traffic and content data in real time.<sup>32</sup> ISPs must also be obliged to keep confidential both the fact of and any information about the collection.<sup>33</sup> The two types of information are differentiated in an important way. It is contemplated that content data will be intercepted only "in relation to a range of serious offenses to be determined by domestic law."<sup>34</sup> The convention encourages signatories to allow the real-time interception of traffic data for the broadest array of offenses.<sup>35</sup>

The significance of this is evidenced by the fact that ISPs are further required to build and maintain an intercept capability on their systems. Aside from the implication of restricting the interception of content data to "serious offenses," the convention is silent as to the standard for such orders. In fact, the convention makes no mention of whether a hierarchical approach to preser-

vation, production or interception orders is preferred. Should one be more or less difficult to justify? Should it depend on the category of information sought? Signatory states are left with considerable discretion in implementing the convention. While privacy is specifically contemplated in the introductory preamble to the convention as an interest to be balanced, it is not referenced in the text of the articles.

It is not unusual for international treaties to be vague in application, given the array of legal systems that must adopt its provisions. It would have been helpful, however, if the convention had outlined in greater detail the nature of the interests affected by the contemplated measures. How should signatories factor privacy or other human rights concerns into the standard for the various orders envisioned? Can or should a state assume that the convention's failure to emphasize privacy rights is indicative of lowered value, when balanced against the international threat of cybercrime?

There are good reasons to favor a restricted application of the convention's measures, in keeping with an overarching framework that values privacy as a fundamental human right. In our view, the convention's terms must be implemented cautiously. Law enforcement should be made to justify preservation and production orders at a very high standard before judicial authorization is granted. These orders should not be available for anticipated crimes, for example, but only when authorities believe that an offense has been committed. Law enforcement should be made to demonstrate that there are reasonable grounds for the order, and the order should be construed as narrowly as possible on a standard of necessity, not relevance, to the investigation. In keeping with our observation that the line between traffic and content data is problematic, the justificatory standard should be the same for both. Finally, if preservation orders are adopted, the convention's suggested time frame of ninety days should be the maximum allowed.<sup>36</sup>

Real-time interception orders are of a different type altogether. Very likely they would warrant separate and more severe treatment. While the convention asks that intercept orders for traffic data be available for a wide variety of offenses, more likely a restricted approach is preferable. As suggested in the discussion of content data, real-time intercept orders of any type should be available only for the most serious offenses under domestic law. They should be narrowly construed, with safeguards to protect and extricate unrelated or innocuous communications. Third-party interests must also be safeguarded. Intercept orders should be granted in exigent circumstances only when other investigatory means are unavailable.

## CONCLUSION

Why require law enforcement to meet such high standards before granting lawful access to our Internet communications? There are two rationales, one individual and one technological. First, we should preserve the integrity of Internet communications, which are becoming a more prominent mode of communication. Individuals use email to communicate with friends, family and business associates. We should be able to expect such interactions to stay private. Given current trends, our reliance on those forms of communication will only become more prevalent. Privacy safeguards must therefore be built into cybercrime legislation, out of respect for individual autonomy and in recognition of the power of technology to create relationships of dependence.

Second, it is a trite observation that once lost, privacy cannot be regained. By treating ISPs as reservoirs of personal information, we fundamentally shift the rela-

tionship between these private entities and those who use them. The proposed legislation not only gives new powers to law enforcement, it also requires ISPs to exercise new discretion and to exercise state like powers. This shift in the regulatory oversight from the public to the private sphere should be legislated more carefully.

Technology is Janus-faced.<sup>37</sup> Just as a stethoscope can be used to hear a beating heart in crisis or to crack a safe, Internet technologies can be used to breathe life into our global village or to trample on individual rights. Our right to privacy is a fundamental human right, one that allows us to define our individuality free from interference by the state and its agents. ISPs have, until recently, helped preserve personal privacy by acting as the stewards of our personal information and private communications. With the Convention on Cybercrime, ISPs will likely be required to shift allegiance to the state. ISPs are required to cooperate with law enforcement and to build and maintain systems of interception and preservation that could result in damaging incursions into user privacy. Privacy protection should be a first-order concern, one that should be contemplated through-out the proposed legislation and entrenched in the text of the convention. Justifications for access to the various categories of investigatory information should be expressly balanced against privacy concerns.

## NOTES

1. Peter Steiner, "On the Internet, Nobody Knows You're a Dog," *The New Yorker*, July 5, 1993, 61.
2. J. Quittner, "Anonymously Yours —An Interview with Johan Helsinguis," *Wired*, Feb. 6, 1994, [http://www.wired.com/wired/archive/2.06/anonymous.1\\_pr.html](http://www.wired.com/wired/archive/2.06/anonymous.1_pr.html) (November 10, 2002).
3. L. Lessig, "The Path of Cyberlaw," 104 *Yale L.J.* 1743 (1995).
4. Tom Toles, "Did You Mark All That?" *Buffalo News*, April 9, 2000, <http://www.ucomics.com/tomtoles>.
5. Associated Press, "Man Charged E-Snooping on Wife," *Wired*, September 6, 2001, <http://www.wired.com/news/privacy/0,1848,46580,00.html> (November 10, 2002); S. Olsen, "Dot-Corns See Gold in Consumer Data," *cxnet News.com*, October 24, 2001, <http://news.com.com/2100-1023-274923.html> (November 10, 2002).
6. Council of Europe, "European Convention on Cybercrime," November 23, 2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (November 10, 2002); Government of Canada (Department of Justice, Industry Canada and Solicitor General), "Lawful Access Consultation Document," August 25, 2002, [http://canada.justice.gc.ca/en/la\\_al/index.html](http://canada.justice.gc.ca/en/la_al/index.html) (November 10, 2002).
7. *R. v. Weir*, 3d 59 *Alta. L.R.*, 319 (*Alta Q.B.* 1998); *R. v. Weir*, 3d 95 *Alta. L.R.* 225 (*Alta. C.A.* 2001).
8. See note 6.
9. See e.g., DePaul University's MIS 680 E-Commerce Fundamentals: <http://www.versaggi.net/e-commerce/disintermediation/> (November 10, 2002).
10. N. Negroponte, "Reintermediated," September 1, 1997, <http://web.media.mit.edu/~nicholas/Wired/WIRED5-09.html> (November 10, 2002).
11. I. Kerr, "Personal Relationships in the Year 2000: Me & My ISP" in *Personal Relationships of Dependence and Interdependence in Law* (Vancouver: UBC Press, 2002).
12. For an elaboration on this point see I. Kerr, "Online Service Providers, Fidelity and the Duty of Loyalty" in *Ethics and Electronic Information: A Festschrift for Stephen Almagno*, ed. B. Rockenback and T. Mendina (Jefferson, NC: McFarland & Co., 2003).
13. See note 7.
14. Recall that the files forwarded to the police were not yet in Mr. Weir's possession, as they had not yet been downloaded to his inbox. This is because his account had been disabled as soon as his available disk quota had been exceeded.
15. Ironically, the warrant upon which the police were authorized to search and ultimately seize Weir's computer was itself founded on emails that he had neither received nor possessed. In fact, it remains unclear whether Weir knew at the time that the emails had been sent to him.
16. See note 7, paragraphs 46 and 49.
17. *R. v. Broyles*, 3 S.C.R. 595 (S.C.C. 1991).
18. See note 17, paragraph 24.
19. See "Lawful Access Consultation Document," note 6.
20. See note 6, Chapter I, Article I, definition d.
21. *Data Mining and Knowledge Discovery*, ed. Usama Fayyad, Heikki Mannila & Raghu Rama-

krishnan (Norwell, MA: Kluwer Academic Publishers, 2002).

22. Signing nations (as of Nov. 10, 2002): Albania (ratified), Armenia, Austria, Belgium, Bulgaria, Canada, Croatia (ratified), Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Malta, Moldavia, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, South Africa, Spain, Sweden, Switzerland, Macedonia, Ukraine, United Kingdom and United States.

23. See note 6, paragraph 6 of preamble.

24. See note 6, paragraphs 8 and 9 of preamble.

25. See note 6, paragraph 7 of preamble.

26. See note 6, paragraphs 10 and 11 of preamble.

27. See note 6, article 16.

28. See note 6, article 16, sec. 1.

29. See note 6, article 17; "Traffic data" are any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

30. See note 6, article 17, sec. 1(b).

31. See note 6, article 18; "Subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which the following can be established: (1) the type of communication service used, the technical provisions taken thereto and the period of service; (2) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and (3) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

32. See note 6, articles 20 and 21.

33. See note 6, article 20, sec. 3 and article 21, sec. 3.

34. See note 6, article 21, sec. 1.

35. See note 6, see article 14, sec. 3(a).

36. Canada's lawful access document raises the consideration of orders of 90, 120 or 180 days. See *Data-Preservation Orders—Issues to Be Considered* available online: [http://canada.justice.gc.ca/en/cons/la\\_al/d.html#15](http://canada.justice.gc.ca/en/cons/la_al/d.html#15) (November 10, 2002).

37. Janus was a Roman god who protected doors and gateways. The god is typically represented in art with two faces looking in different directions, symbolic of entrances and departures through the gateway. Janus also represented beginnings, thus the first month of our year is named "January."