BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Internet

Online Privacy

The use of deep packet inspection (DPI) allows service providers to look ''inside'' each transmission packet and inspect all data and information contained in it. The use of DPI presents some unsettled legal questions, most notably, does automated scanning of users' Web communications result in ''interceptions'' that implicate federal and state wiretapping laws, and, if so, in what circumstances, if any, would such ''interceptions'' be lawful? Samir Jain of WilmerHale writes that those issues provide a helpful lens through which to consider whether targeted advertising, content filtering, and network management practices might violate users' reasonable expectations of privacy in their online communications.

The Promise and Perils of Deep Packet Inspection

BY SAMIR JAIN

Jain is a partner in the Communications and E-Commerce group at WilmerHale, in Washington. He has extensive experience advising clients and litigating cases in areas such as network security and electronic surveillance, privacy, and online content liability. The views expressed in this article are his own and do not necessarily reflect those of his clients.

As a new Administration and Congress settle into office, a number of highly charged online privacy controversies appear to be on the legislative and regulatory agenda. They include issues such as whether broadband service providers should be permitted to target advertising based on a subscriber's online behavior (e.g., sites visited and searches conducted); whether service providers can detect and block attempts to access or exchange unlawful content such as child pornography or, more controversially, music and video that infringe copyrights; and whether service providers should be able to monitor and ''manage'' traffic on their

networks or should be subject to ''net neutrality'' rules that prohibit or restrict such practices.

Although these issues each present a different set of policy considerations, they also have a common thread. In each case, a broadband service provider would play a gatekeeping role requiring it to monitor and analyze the traffic traversing its network in a more detailed manner than needed merely to route traffic from the content originator to the intended recipient(s). A service provider can accomplish this task through what is termed ''deep packet inspection,'' or DPI. As the name implies, deep packet inspection allows the service provider to look ''inside'' each packet and inspect all data and information contained in it. The use of DPI presents some unsettled legal issues. Most notably, does automated scanning of users' Web communications in this way result in ''interceptions'' of those communications that implicate federal and state wiretapping laws, and, if so, in what circumstances, if any, would such ''interceptions'' be lawful? Analyzing that issue provides a helpful lens through which to consider whether targeted advertising, content filtering, and network management practices might violate users' reasonable expectations of privacy in their online communications.

What is deep packet inspection? A packet is often conceptualized as having two parts: a ''header'' (analogous to an envelope) and a data or payload portion (analogous to what is contained in the envelope). In the normal course of simply routing packets over its network, a broadband service provider need only look at the ''header'' portion of the packet, which includes information such as the sender's and recipient's IP addresses and protocol and other formatting information. In the case of DPI, however, the service provider can ''inspect'' the entire packet, including the data portion. Notably, deep packet inspection is not a technique for breaking encryption, so data sent in encrypted form remains secure.

Of course, given the volume of packets at issue, DPI must as a practical matter be done in automated form, at least in the first instance (depending on the purpose of for which the service provider is using DPI, certain packets might be blocked or held for further analysis and a person might then become aware of the contents of such packets). Thus, for example, a provider could install hardware and software at various points on its network and place an incoming packet in a buffer as it passed through one of those checkpoints. The packet could then be analyzed to determine whatever information was needed to carry out the purpose of the DPI (e.g., whether the complete URL contained in the packet matched a blacklist of URLs known to display child pornography). Then, depending on the results of that analysis, the packet would continue on its route—perhaps with some information about its contents or other attributes being recorded—or be blocked or diverted.

Does deep packet inspection result in the ''interception'' of communications for purposes of the federal Wiretap Act? With various exceptions, the federal Wiretap Act generally prohibits the intentional interception of an electronic communication, as well as the disclosure or use of the contents of an unlawfully intercepted communication.[1] The Act defines an ''intercept'' as ''the *aural or other acquisition* of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.''[2] Thus, two key issues are whether DPI amounts to an ''aural or other acquisition'' and, if so, whether the information being acquired is the ''contents'' of the communication.

The Wiretap Act does not itself define the term ''acquisition.'' Its common meaning is ''the gaining of possession or control over something.''[3] Thus, for example, courts have held that making a recording or copy of a communication can amount to its ''acquisition.''[4] Thus, one relevant question in assessing whether a particular implementation of DPI results in acquisition is whether a copy or other recording of the packet is made, and whether, if it is just a transient copy to permit analysis of the packet that is then immediately deleted, that transient copy is enough to constitute acquisition.

Even absent creation of a copy, one might argue that automated scanning of packets as they traverse the network itself constitutes ''acquisition.'' After all, a person listening to a conversation engages in ''aural acquisition'' even if no recording or copy is made. Does the fact that it is instead a computer ''listening'' to the packets as they go by make a decisive difference? The case law has not definitively addressed the question whether automated scanning of a communication amounts to an acquisition. A few cases could be read to suggest that it does not. For example, in a U.S. Court of Appeals for the D.C. Circuit case from the 1970s, the plaintiffs alleged that National Security Agency computers ''scan[ned]'' communications using ''watchlists'' of words and phrases to select particular communications for review by intelligence analysts. The plaintiffs, whose names were on the watchlists, brought claims for unlawful interception of their communications. The court rejected ''the plaintiff's argument that the acquisition of a plaintiff's communications could be presumed from the existence of a name on the watchlist'' and held that, to establish that their calls were ''acquired,'' plaintiffs would need to prove not just that their communications were scanned but that their calls were selected by the computer for human examination.[5] A Fourth Circuit case similarly concluded that even where a device provides access to communications and thereby puts one in the position to acquire the communication, no interception occurs if the contents of the communications are not actually ''acquired'' by listening to, recording, or otherwise preserving them.[6]

---

[1] 18 U.S.C. § 2511(1).

[2] 18 U.S.C. § 2510(4) (emphasis added).

[3] Black's Law Dictionary (8th ed. 2004); *see also* Webster's Third (defining ''acquire'' as ''to get as one's own; to come into possession or control of . . . .'').

[4] *See, e.g.*, *United States v. Lewis,* 406 F.3d 11, 17 n.5 (1st Cir. 2005) (rejecting argument that acquisition of contents of call did not occur until recordings were listened to); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994) (''The recording of a telephone conversation alone constitutes an ''aural . . . acquisition'' of that conversation.''); *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994) (holding that ''systematic recording of phone conversations falls squarely under the definition of 'intercept' '' even if no one hears the communication).

[5] *See Halkin v. Helms*, 598 F.2d 1, 11 (D.C. Cir. 1978).

[6] *See Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 739, 742 (4th Cir. 1994) (holding that no interception occurred when a live microphone picked up sounds and voices in the plaintiff's office and transmitted them to the defendant's security control room and rejecting argument that Wiretap Act ''does not re-

  PVLR ISSN 1538-3423

This case law arguably suggests that automated scanning or ''inspection'' of packets as they pass through a network without making a copy or other record would not amount to an ''acquisition.'' Nevertheless, there remains significant uncertainty about how a court would decide this question if confronted with the facts related to implementation of DPI or its equivalent. A court offended by DPI could conceptualize the process as one in which the packets are ''acquired'' temporarily—during the brief moment in which they are ''stopped'' or slowed down to be inspected—perhaps by analogy to cases that have construed ''intercept'' as involving the ''capture'' or ''redirection'' of a communication.[7]

Even if a court were to determine that DPI involves ''acquisition,'' in order to find that there was an interception, it would also need to conclude that what was acquired was the ''contents'' of a communication. The Wiretap Act defines ''contents'' as ''any information concerning the substance, purport, or meaning'' of ''any wire, oral, or electronic communication.''[8] Courts have held that ''contents'' can include not only, for example, the text of e-mail messages,[9] but also the subject lines of messages[10] or bank account and credit card numbers entered by a website visitor during a transaction.[11] By contrast, the term ''contents'' does not include information about electronic communications that facilitates the routing of electronic communications: ''contents do not include 'dialing, routing, addressing, or signaling information' relating to the delivery and nature of wire and electronic communications.''[12] This type of information, such as an Internet protocol address, functions much like a phone number by designating the computer a user is trying to reach. The definition of ''contents'' in the Wiretap Act also does not include transactional records about a communication. Congress specifically amended the definition of contents in 1986 ''to exclude from the definition of the term 'contents,' the identity of the parties or the existence of the communication. It thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it.''[13]

Whether DPI implicates the statutory term ''contents'' likely will turn on the particular facts and the purpose for which it is being used. One could argue that simply identifying the *type* of traffic (e.g., that the packet is associated with a peer-to-peer communication) does not reveal information about the meaning, substance, or purport of the communication, at least if such identification did not require determining what file was being exchanged or whether the file was a song, movie, or some other form of content. This argument would be strengthened to the extent that the type of traffic might affect how it is routed. For example, if Voice over Internet Protocol traffic were identified for the purpose of assigning it higher priority for routing purposes, that would tend to support the conclusion that determining whether a packet was part of a VoIP communication should not be deemed to constitute acquiring its contents.

Conversely, using DPI to block access to illegal content might implicate contents in certain cases where such filtering was done using the full URL and not just the portion used to determine the IP address of the destination. In some cases, the full URL includes information provided by the user. For example, if a website uses the ''get method'' to obtain information about what file or data a user is seeking, the information provided by the user is appended to the end of the URL. Likewise, when a user engages in a search on a site such as Google, the search query is appended to the URL. In at least some contexts, courts have held that user-generated information that becomes part of a website URL is ''contents'' under the Wiretap Act. For example, the First Circuit concluded that a defendant recorded ''contents'' when it captured information (such as search terms associated with a user's medical condition'') that was ''appended to the query string at the end of the URL of the webpage showing the search results.''[14] Similarly, the U.S. District Court for the District of Massachusetts held that if an Internet user ''enters a search phrase'' in a search engine and ''that search phrase [appears] in the URL after the first forward slash,'' this ''would reveal . . . information concerning the substance, purport or meaning of that communication.' ''[15]

In sum, whether DPI results in interception of communications remains an unsettled question at virtually every turn.[16] Moreover, the answer may not be the same for every implementation of DPI: it may depend on the particular way in which the DPI at issue works and what information, if any, is being captured and for what reason.

Even if deep packet inspection results in interception, would an exception apply? As noted earlier, even while

quire proof of listening or of preservation for listening purposes'').

[7] *See, e.g.*, *United States v. Hammond*, 286 F.3d 189, 193 (4th Cir. 2002) (noting that the term ''intercept'' in Title III ''clearly operates in terms of a '*capture*' concept,'' and that ''an interception is something that is *obtained* and *held*'' (emphasis added)); *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992) (''It seems clear that when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time.'').

[8] 18 U.S.C. § 2510(8).

[9] *Mink v. Salazar*, 344 F. Supp. 2d 1231 (D. Colo. 2004).

[10] *In re Application of the United States for an Order Authorizing Use of a Pen Register*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005).

[11] *Id.*

[12] LaFave et al., CRIMINAL PROCEDURE § 4.6(b) (3d ed.) (2008) (citing 18 U.S.C. § 3127(3)-(4)); *see also In re Application.*, 396 F. Supp. 2d at 47 (''dialing, routing, addressing, or signaling information'' does not constitute ''contents'' for purposes of the Wiretap Act unless they reveal the contents of a communication).

[13] S. Rep. No. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.

[14] *In re Pharmatrak Privacy Litig.*, 329 F.3d 9, 16, 18 (1st Cir. 2003).

[15] *In re Application of United States for an Order Authorizing Use of a Pen Register*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

[16] Additional uncertainties abound. For example, the Wiretap Act defines ''intercept'' as occurring ''through the use of any electronic, mechanical, or other device.'' 18 U.S.C. § 2510(4). An ''electronic, mechanical, or other device'' is then defined as ''any device or apparatus which can be used to intercept a wire, oral, or electronic communication *other than . . . any telephone or telegraph instrument, equipment or facility*, or any component thereof . . . *being used by a provider of wire or electronic communication service in the ordinary course of its business . . .*'' 18 U.S.C. § 2510(5) (emphasis added). Depending on the facts, the use of DPI could fall within this definitional carve-out.

federal and state wiretap laws generally prohibit interception of another's communications, the statutes have a number of exceptions, at least two of which might apply to DPI.

In sum, whether DPI results in interception of communications remains an unsettled question at virtually every turn.

One exception permits a service provider to intercept a subscriber's communication ''while engaged in any activity which is a necessary incident to the rendition of [its] service or to the protection of the right or property of the provider of that service.''[17] The large majority of published cases addressing the ''protecting the right or property'' prong of the provider exception arise in a context where providers ''intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of [their own] service.''[18] It is less clear that the exception would apply to interceptions used to gather information concerning a crime that was unrelated to a provider's own rights or property.[19] Thus, for example, DPI used for the purpose of filtering unlawful content may not fall within this exception, at least absent some reason to believe that the service provider was itself at risk for liability because it was carrying that content. But there are close cases that have yet to be tested: for example, a service provider might argue that its reputation is harmed to the extent that illegal content, particularly heinous content such as child pornography, is accessible through its service, and that preventing such damage is protecting its rights or property.

Under the second prong of the provider exception—where surveillance is a ''necessary incident to the rendition of his service''—a provider does not incur liability where the intercept is unavoidable in the ordinary course of business. For example, a repairman who overhears a conversation when tapping phone lines in the course of completing repairs does not violate the Wiretap Act.[20] Interception activity may fall within this exception where it is done to maintain service quality. Thus, using DPI to detect VoIP traffic so as to prioritize its handling and limit problems such as latency might be permissible under this exception. Similarly, use of DPI to detect peer-to-peer traffic might fall within the incident to the provision of service exception if it were used for quality control, routing, or similar purposes relating to how the service was provided.

A second exception under the Wiretap Act permits an interception if at least one party to the communication consents.[21] Thus, a service provider might attempt to obtain consent for DPI through, for example, its terms of service. Although in many respects, this is an appealing solution, the disclosures necessary to ensure that a subscriber could reasonably be said to have been on notice and consented to DPI activities might, as recent controversies attest, raise significant concerns on the part of both the public and regulators. Even leaving that aside, relying on consent raises at least two other issues. First, although federal law requires the consent of only one party, a number of state laws require consent of all parties to a communication. Yet a service provider presumably could not obtain consent from a nonsubscriber who talks to one of its own subscribers using VoIP or a third-party website with which a subscriber is communicating. Second, even with respect to its own subscribers, it is not clear whether consent on the part of the subscriber would be sufficient to constitute consent for all members of the subscriber's household: in other words, if a husband registers for broadband service and consents to deep packet inspection but does not tell his wife, she may not be deemed to have consented to interception of all her VoIP calls.

* * *

As this discussion suggests, the complexity of the applicable Wiretap Act provisions and the various possible fact patterns makes it difficult to definitively answer the question whether the use of DPI violates existing wiretapping laws. But that uncertainty also reflects the lack of settled understandings concerning the underlying policy question: namely, what reasonable expectations of privacy can and should users have concerning online communications and activities. One court, in a decision subsequently vacated and taken en banc, stated outright that ''[t]he fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content.''[22] Others, however, are offended by the notion that a service provider might inspect all of their online communications, even if only in an automated way. The debate over DPI can be settled only by reaching some rough consensus about whether and in what circumstances service providers should be permitted to act as gatekeepers of our online communications and activities

[17] 18 U.S.C. § 2511(2)(a)(i).

[18] *United States v. Villanueva*, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998); *United States v. Harvey*, 540 F.2d 1345, 1352 (8th Cir. 1976) (exception was ''designed to allow the disclosure of justified wire monitoring by communications carriers for the purpose of criminal prosecution of those who fraudulently use their services.'').

[19] *Hodge v. Mountain States Telephone and Telegraph Co.*, 555 F.2d 254 (9th Cir. 1977) (declining to apply provider exception to investigation into obscene telephone calls).

[20] *United States v. Ross*, 713 F.2d 389, 392 (8th Cir. 1983); *United States v. Savage*, 564 F.2d 728, 731-32 (5th Cir. 1977) (telephone operator receiving telephone calls in the normal course of her employment inevitably overhears a portion of the call).

[21] 18 U.S.C. § 2511(2)(d).

[22] *See Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *rev'd*, 532 F.3d 521 (6th Cir. 2008) (en banc).

  PVLR ISSN 1538-3423