

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

In re INNOVATIO IP VENTURES, LLC	)	
PATENT LITIGATION	)	
	)	MDL Docket No. 2303
THIS ORDER APPLIES TO ALL CASES	)	Case No. 11 C 9308
Pretrial Order No. 6	)	
	)	

MEMORANDUM OPINION AND ORDER ADDRESSING PROTOCOL FOR  
INNOVATIO’S WI-FI “SNIFFING”

JAMES F. HOLDERMAN, Chief Judge:

Plaintiff Innovatio IP Ventures, LLC (“Innovatio”) has sued various hotels, coffee shops, restaurants, supermarkets, and other commercial users of wireless internet technology located throughout the United States (collectively, the “Wireless Network Users”). (*See* Dkt. No. 198 (“Second Am. Compl.”).) Innovatio alleges that, by making wireless internet available to their customers or using it to manage internal processes, the Wireless Network Users infringe various claims of seventeen patents owned by Innovatio. (*Id.* ¶¶ 48-81.) In addition, several manufacturers of the products that the Wireless Network Users use to provide wireless internet (collectively, the “Manufacturers”) have brought declaratory judgment actions against Innovatio seeking a declaration that their products, and the networks or systems of which they are a part, do not infringe Innovatio’s patents. *See* Compl. (Dkt. No. 1), *Cisco Sys., Inc. v. Innovatio IP Ventures*, No. 11-cv-9309 (N.D. Ill. May 13, 2011). All claims and parties were consolidated before this court by the Judicial Panel on Multidistrict Litigation. (Dkt. No. 1.) Pending before the court is Innovatio’s motion titled “Rule 16(c)(2) Motion for Entry of Protocol for Collection of Electronic Evidence and Preliminary Ruling on Admissibility of Evidence Collected Therefrom.” (Dkt. No. 329.) For the reasons explained below, that motion is granted.

## BACKGROUND

The standard for the operation of wireless networks that access the internet is established by the Institute of Electrical and Electronic Engineers (“IEEE”), and is known as IEEE 802.11, or “Wi-Fi.” As discovery has proceeded in this case, Innovatio has been using commercially-available Wi-Fi network analyzers to collect information about the Wireless Network Users’ allegedly infringing Wi-Fi networks. (Dkt. No. 329, at 2.) That process, which is known in the industry as “sniffing,” requires Innovatio’s technicians to enter the Wireless Network Users’ premises during business hours with a laptop computer and a Riverbed AirPcap Nx packet capture adapter (or a similar device). (*Id.*) The packet capture adapter can intercept data packets that are traveling wirelessly between the Wi-Fi router provided by the Wireless Network Users and any devices that may be communicating with it, such as a customer’s laptop, smartphone, or tablet computer. Innovatio then uses Wireshark network packet analyzer software to analyze the data packets, revealing information about the configuration of the network and the devices in the network. The data packets also include any substantive information that customers using the Wi-Fi network may have been transmitting during the interception of the data packets, including e-mails, pictures, videos, passwords, financial information, private documents, and anything else a customer could transmit to the internet. Innovatio contends that the information it collects will assist in proving its infringement claims.

Before continuing to incur the expense of additional sniffing, Innovatio sought permission to obtain a preliminary ruling on the admissibility of the information that it gains in the sniffing process. (Dkt. No. 290.) The court granted permission to Innovatio to seek an admissibility ruling (Dkt. No. 323), but expressed some concern that Innovatio’s sniffing may implicate the privacy interests of the customers using the Wi-Fi networks under the federal Wiretap Act. 18 U.S.C.

§§ 2510-2522. Accordingly, the court ordered Innovatio's motion to describe its proposed sniffing protocol in detail and to address the applicability of the Wiretap Act. Innovatio has submitted a proposed protocol under seal (Dkt. No. 329, Ex. A), and now requests that the court approve that protocol and issue a preliminary ruling on the admissibility of any evidence Innovatio may gather through the use of that protocol.

### ANALYSIS

#### **I. The Federal Wiretap Act**

The Federal Wiretap Act provides that, with certain exceptions, “any person who . . . intentionally intercepts . . . any wire, oral, or electronic communication” shall be subject to criminal and civil liability. 18 U.S.C. § 2511(1)(a); *see also* 18 U.S.C. § 2520(a). An “electronic communication” includes “any transfer of signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” Neither party disputes that the allegedly infringing Wi-Fi networks transmit information using radio waves (which are a type of electromagnetic radiation), and thus transmit “electronic communications.”

Nonetheless, Innovatio contends that the Wiretap Act does not apply because it has altered the source code of the Wireshark software so that it no longer intercepts the contents of any third-party communication.<sup>1</sup> The Wiretap Act provides that “‘intercept’ means 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.” 18 U.S.C. § 2510(4). The “contents” of a communication

---

<sup>1</sup> At least some of Innovatio's initial sniffing efforts proceeded with an unmodified version of the software that did preserve the contents of the wireless communications.

are “any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8). According to Innovatio, its modified Wireshark software “overwrites the data payload (i.e. the ‘substance’ of the [Wi-Fi] communication) before the results are provided to the user,” while still collecting the header information that it needs to analyze the configuration of the wireless network (such as the source of the data packet, the destination of the packet, the packet length, and the checksum<sup>2</sup>). (Dkt. No. 329, at 4.) Innovatio thus contends that it is not acquiring the contents of any communication, and that its sniffing does not violate the Wiretap Act.

In response, the defendants<sup>3</sup> argue that the process of “overwriting” the data payload implies that Innovatio initially captures the data payload before deleting it. According to the defendants’ expert, James Edward Hung, the mere act of initially recording the data payload is sufficient to complete the acquisition of the data, regardless of whether the intercepted data is later overwritten before it is used. (Dkt. No. 349, Ex. 5 (“Hung Decl. ¶ 12).) The defendants thus contend that Innovatio’s proposed protocol intercepts the contents of the communication. In support of that argument, the defendants note that § 2511(1)(d) of the Wiretap Act contains a separate provision prohibiting the *use* of intercepted communications and that, to avoid redundancy with that section, § 2511(1)(a)’s prohibition on interception must not require the use of the communication as an element of the offense. *See Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (“No new interception occurs when a person listens to or copies the communication that has already been captured or

---

<sup>2</sup> The checksum is the output of an algorithm that is run on a data packet both before and after transmission to ensure that the data packet has not been corrupted. (Dkt. No. 384, at 5 n.4.) If the algorithm produces the same output both before and after transmission, the data packet is deemed valid; otherwise, it is discarded as corrupt. (*Id.*)

<sup>3</sup> The court uses the term “defendants” to refer collectively to both the Wireless Internet Users and the Manufacturers, who are technically declaratory judgment plaintiffs.

redirected. Any subsequent use of the recorded conversation is governed not by the prohibition on interception, but by the prohibition in § 2511(c) and (d) on the ‘use’ and ‘disclos[ure]’ of intercepted wire communications.”).

Innovatio replies, however, that the defendants have misunderstood the relevant technology. According to Innovatio’s expert, Ray Nettleton, all Wi-Fi devices necessarily store an entire received data packet, including the packet’s substantive communications, while the device processes the packet. (Dkt. No. 384, Ex. U (“Nettleton Decl.”) ¶ 40.) During processing, if the Wi-Fi device determines that the data packet is not addressed to it or has been corrupted during transmission, the packet is deleted. (*Id.* ¶¶ 42-46.) Prior to that point, the entire data packet is retained only in the Wi-Fi device’s random access memory, and is not stored in a permanent medium. (*Id.* ¶ 47.) The entire process is momentary, so deleted packets are retained in memory for no more than milliseconds. (*Id.* ¶ 48.) Innovatio proposes to automatically overwrite all substantive communications in the data packets that it intercepts, making its protocol “intercept” substantive communications only to the extent that a normal Wi-Fi device would intercept all communications on a Wi-Fi network to which it is connected. (*Id.* ¶ 54.) If its proposal runs afoul of the Wiretap Act, Innovatio argues, then all Wi-Fi devices necessarily violate the Act whenever they are connected to a Wi-Fi network that also includes devices belonging to a another party, an absurd result.

In essence, Innovatio asks the court to conclude that a communication is not “intercepted” until it has been recorded in a permanent medium. The court is hesitant to adopt that conclusion, first because that requirement is nowhere found in the Wiretap Act. Moreover, an individual’s online activity can be chilled merely by the knowledge that a third party has the power to acquire, however briefly, the contents of his communications. *See Amati v. City of Woodstock*, 829 F. Supp. 998, 1008

(N.D. Ill. 1993) (holding that the privacy interests of an individual whose conversations come under the power of another are implicated “even if the individual was assured no one would listen to his conversations, because the individual’s privacy interests are no longer autonomous”); *see also United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992) (acquisition occurs “when the contents of a wire communication are captured or redirected *in any way*” (emphasis added)).

The court need not, however, construe the term “intercept” in this case, nor must it resolve the dispute between the parties’ experts. The reason is that, even assuming that Innovatio’s proposed protocol intercepts Wi-Fi communications, Innovatio’s proposed protocol falls into the exception to the Wiretap Act allowing a person “to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.” 18 U.S.C. § 2511(g)(i).<sup>4</sup> Most of the Wireless Network Users’ Wi-Fi networks are open and available to the general public, allowing any customer who so desires to access the internet through them. The question is not, however, whether the *networks* are “readily available to the general public,” but instead whether the network is configured in such a way so that the *electronic communications* sent over the network are readily

---

<sup>4</sup> Innovatio also contends that the defendants and their customers have consented to Innovatio’s sniffing efforts. Although the defendants agreed that “Innovatio may use commercially-available network analyzers to collect information allegedly regarding the identity (e.g., SSID, manufacturer and MAC address), configuration and use of the allegedly infringing networks” (Dkt. No. 218 ¶ 9), however, they did not consent to allowing Innovatio to collect the substantive communications sent over the Wi-Fi networks. As for the customers, Innovatio presents evidence that several of the defendants require customers to agree to a waiver of privacy rights before accessing the defendants’ Wi-Fi networks. (Dkt. No. 329, at 7; Dkt. No. 384, at 9-13.) There is no evidence about how many of the defendants require such a waiver, however, nor does Innovatio provide legal analysis of the language of each waiver to determine if it waives the protections of the Wiretap Act against the sniffing of a third party. The court will not merely assume that all defendants require customers to agree to language waiving the protections of the Wiretap Act.

available.

The only reported decision addressing that question is *In re Google Inc. Street View Electronic Communications Litigation*, 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011). In that case before Chief Judge Ware, the plaintiffs sued Google under the Wiretap Act for the intentional interception of data from their unencrypted home Wi-Fi networks during the collection of data for the Google Street View feature of Google Maps. In denying Google's motion to dismiss, the court noted that the plaintiffs had alleged that the data packets transmitted over the Wi-Fi networks "were not readable by the general public without the use of sophisticated packet sniffer technology." *Id.* at 1082. After accepting that allegation as true, the court held that the data packets were not readily accessible to the general public:

[C]ommunications sent via Wi-Fi technology, as pleaded by Plaintiffs, are not designed or intended to be public. Rather, as alleged, Wi-Fi technology shares a common design with cellular phone technology, in that they both use radio waves to transmit communications, however they are both designed to send communications privately, as in solely to select recipients, and both types of technology are architected in order to make intentional monitoring by third parties difficult.<sup>5</sup>

The court's conclusion thus depended on the proposition that data packets sent through unencrypted Wi-Fi networks are only readable with "sophisticated packet sniffer technology," a proposition that the court accepted as true under the standards applicable to a motion to dismiss.

---

<sup>5</sup> *Id.* The court rejected the argument that "readily available to the general public" should be defined according to the definition in 18 U.S.C. § 2510(16), which defines the phrase "with respect to a radio communication." Although Wi-Fi networks operate through the use of radio waves, the court held that the definition applies to only "traditional radio services," and not to Wi-Fi technology. *Id.* at 1081. The defendants do not argue that the § 2510(16) definition should apply here. The court thus assumes, without deciding, that § 2510(16) does not apply in this case, and that the court should give the phrase "readily available to the general public" its ordinary meaning. *Hamilton v. Lanning*, 130 S. Ct. 2464, 2471 (2010) ("When terms used in a statute are undefined, we give them their ordinary meaning." (quoting *Asgrow Seed Co. v. Winterboer*, 513 U.S. 179, 187 (1995))).

Here, by contrast, the court is not required to accept any such allegation. Moreover, upon examination, the proposition that Wi-Fi communications are accessible only with sophisticated technology breaks down. As mentioned above, Innovatio is intercepting Wi-Fi communications with a Riverbed AirPcap Nx packet capture adapter, which is available to the public for purchase for \$698.00. *See Riverbed Technology Product Catalog*, <http://www.cacotech.com/products/catalog/> (last visited Aug. 21, 2012). A more basic packet capture adapter is available for only \$198.00. *Id.* The software necessary to analyze the data that the packet capture adapters collect is available for download for free. *See Wireshark Frequently Asked Questions*, <http://www.wireshark.org/faq.html#sec1> (last visited Aug. 21, 2012) (“Wireshark® is a network protocol analyzer. . . . It is freely available as open source . . . .”). With a packet capture adapter and the software, along with a basic laptop computer, any member of the general public within range of an unencrypted Wi-Fi network can begin intercepting communications sent on that network. Many Wi-Fi networks provided by commercial establishments (such as coffee shops and restaurants) are unencrypted, and open to such interference from anyone with the right equipment. In light of the ease of “sniffing” Wi-Fi networks, the court concludes that the communications sent on an unencrypted Wi-Fi network are readily available to the general public.

To be sure, the majority of the public is likely unaware that communications on an unencrypted Wi-Fi network are so easily intercepted by a third party. *See* Predrag Klasnja et al., “*When I Am on Wi-Fi, I am Fearless: Privacy Concerns & Practices in Everyday Wi-Fi Use*, in CHI '09 PROC. 27TH INT'L CONF. (2009), available at <http://appanalysis.org/jjung/jaeyeon-pub/FormativeUserStudy4CHI.pdf> (reporting the results of a study involving eleven participants and concluding that “users from the general public . . . were largely unaware of . . . the visibility of



unencrypted communications,” which “led them to a false sense of security that reduced how much they thought about privacy and security while using Wi-Fi”); *see also* Press Release, Wi-Fi Alliance, *Wi-Fi Security Barometer Reveals Large Gap Between What Users Know and What They Do* (Oct. 5, 2011) (reporting that only 18% of users take steps to protect their communications when accessing a commercial Wi-Fi hotspot). The public still has a strong expectation of privacy in its communications on an unencrypted Wi-Fi network, even if reality does not match that expectation.

The public’s lack of awareness of the ease with which unencrypted Wi-Fi communications can be intercepted by a third party is, however, irrelevant to a determination of whether those communications are “readily available to the general public.” 18 U.S.C. § 2511(g)(i). The language of the exception does not, after all, refer to “communications that the general public knows are readily available to the general public.” Therefore, the public’s expectation of privacy in a particular communication is irrelevant to the application of the Wiretap Act as currently written. Because data packets sent over unencrypted Wi-Fi networks are readily available using the basic equipment described above, the Wiretap Act does not apply here. Accordingly, to the extent that Innovatio’s proposed sniffing protocol accesses only communications sent over unencrypted Wi-Fi networks available to the general public, it is permissible under § 2511(g)(i)’s exception to the Wiretap Act.<sup>6</sup>

Any tension between that conclusion and the public’s expectation of privacy is the product of the law’s constant struggle to keep up with changing technology. Five or ten years ago, sniffing

---

<sup>6</sup> The parties argue briefly in footnotes about whether Innovatio should be allowed to sniff the defendants’ private networks that are not available to the public. (*See* Dkt No. 329, at 5-6 n.3; Dkt. No. 349, at 8 n. 6.) The court declines to address that question at this time because the protocol that Innovatio has moved the court to approve applies by its terms only to “Public-facing Networks.” (Dkt. No. 329, Ex. A.) In approving that protocol, therefore, the court need not address the propriety of sniffing private networks. If Innovatio desires to sniff private networks, the court encourages the parties to confer and to attempt to agree on an appropriate protocol for that activity.

technology might have been more difficult to obtain, and the court's conclusion might have been different. But it is not the court's job to update the law to provide protection for consumers against ever changing technology. Only Congress, after balancing any competing policy interests, can play that role. Indeed, one United States Senator has already called for changes to the Wiretap Act in light of the threat that unencrypted communications may be easily intercepted. *See Elec. Privacy Info. Ctr., On Google Spy-Fi, Senator Durbin Calls for Update to Wiretap Law, FCC Chair Agrees Law Should Protect Unencrypted Communications* (May 11, 2012), <http://epic.org/2012/05/on-google-spy-fi-senator-durbi.html>. Unless and until Congress chooses to amend the Wiretap Act, the interception of communications sent over unencrypted Wi-Fi networks is permissible.

## **II. The Pen Registers and Trap and Trace Devices Act**

The defendants also briefly contend that Innovatio's proposed protocol violates the Pen Registers and Trap and Trace Devices Act. 18 U.S.C. §§ 3121-3127. That statute makes it a crime to "install or use a pen register or a trap and trace device." 18 U.S.C. § 3121(a). A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(3). A trap and trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(4).

The defendants' argument is a single paragraph, and it cites no cases applying the Pen Registers and Trap and Trace Devices Act to Wi-Fi packet capture adapters. Because all Wi-Fi devices on a network necessarily receive addressing information to determine if a data packet is addressed to them, doing so would put any user of a Wi-Fi network on which a third party was also operating in violation of the Act. Moreover, there is some doubt that the Pen Registers and Trap and Trace Devices Act applies to any device that is also capable of collecting the contents of a communication. *In Matter of Application of U.S. For an Order Authorizing the Installation & Use of a Pen Register & a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 18 (D.D.C. 2006) (“[P]en registers’ and ‘trap and trace devices’ are statutorily defined as processes or devices that are prohibited from collecting ‘the contents of any communication.’ 18 U.S.C. § 3127(3)-(4). Consequently, the argument could be made that any process or device that collects the *content* of an electronic communication is not, in fact, a pen register or trap and trace device but, instead, is an electronic intercepting device as defined in [the Wiretap Act].”). Operating as it is without adequate briefing on the subject, the court declines to apply the Pen Registers and Trap and Trace Devices Act to Wi-Fi packet capture adapters.


### **III. The Admissibility of the Information Innovatio Collects**

In light of the court's conclusion that Innovatio's proposed sniffing protocol does not violate the Wiretap Act or the Pen Registers and Trap and Trace Devices Act, the evidence Innovatio collects through the use of that protocol will not be inadmissible because of a violation of those Acts. Accordingly, if Innovatio lays a proper foundation under the Federal Rules of Evidence at trial for the information it collects through the sniffing protocol, that evidence will be admissible.

### CONCLUSION

Innovatio's "Rule 16(c)(2) Motion for Entry of Protocol for Collection of Electronic Evidence and Preliminary Ruling on Admissibility of Evidence Collected Therefrom" (Dkt. No. 329) is granted. Innovatio may collect information from the defendants' public-facing Wi-Fi networks according to its proposed protocol. (Dkt. No. 329, Ex. A.)

ENTER:

A handwritten signature in black ink that reads "James F. Holderman". The signature is written in a cursive style with a large initial 'J'.

-----  
JAMES F. HOLDERMAN  
Chief Judge, United States District Court

Date: August 22, 2012