Case No. 11-17483

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BENJAMIN JOFFE, *et al.*,
Plaintiffs-Appellees,

v.

GOOGLE INC.,
Defendant-Appellant

On Appeal from the United States District Court
for the Northern District of California, Case No. 5:10-MD-2184-JW
Hon. James Ware, U.S. District Judge

BRIEF OF AMICUS CURIAE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION IN SUPPORT OF GOOGLE'S PETITION FOR REHEARING AND REHEARING EN BANC

ASHOK RAMANI
MICHAEL S. KWUN
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111-1809
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

Counsel for Amicus Curiae
Information Technology & Innovation
Foundation

October 4, 2013

Table of Contents

Table of Authorities

Page(s)

Federal Statutes

Federal Rules

Other Authorities

I. STATEMENT OF INTEREST

The Information Technology and Innovation Foundation ("ITIF") files this brief[1] to inform the Court of the devastating consequences its ruling will have on all aspects of the economy that rely on wireless technology infrastructure, including but not limited to healthcare, financial institutions, retailers, and residential computer users; and further to explain the erroneous assumptions of technological fact that form the basis for the Court's holding that an unencrypted Wi-Fi communication is not readily accessible to the general public.

ITIF, a 501(c)(3) nonprofit organization founded in 2006, is a non-partisan research and educational institute—a think tank. Its mission is to formulate and promote public policies to advance technological innovation and productivity internationally, in Washington, and in the states. Recognizing the vital role of technology in ensuring prosperity, ITIF focuses on innovation, productivity, and digital economy issues.

ITIF believes that technological innovation, particularly in information technology, is at the heart of America's growing economic prosperity. ITIF further believes that crafting effective policies that boost innovation and encourage the

[1] All parties have consented to the filing of this brief. Fed. R. App. P. 29(a); Circuit Rule 29-2(a). None of the parties to this case or their counsel authored this brief in whole or in part. No party or their counsel contributed money intended to fund preparing or submitting the brief. No one else other than ITIF and its counsel contributed money that was intended to fund preparing or submitting this brief.

widespread "digitization" of the economy is critical to ensuring robust economic growth and an improved standard of living. ITIF's mission is to help policy makers at the federal and state levels to better understand the nature of the new innovation economy and the types of public policies needed to drive innovation, productivity and broad-based prosperity for all Americans.

ITIF publishes policy reports, holds forums and policy debates, advises elected officials and their staff, and is an active resource for the media. Among other things, ITIF also analyzes existing policy issues through the lens of advancing innovation and productivity, and opposes policies that hinder digital transformation and innovation.

Consistent with its mission and its other work, ITIF files this brief to urge the Court to avoid interpreting the Wiretap Act in a way that would needlessly call into legal question standard information technology practices, based on incorrect assumptions of technological fact.

II. SUMMARY OF ARGUMENT

A. The issue presented and the Court's holding.

Under the Wiretap Act, one who intentionally intercepts an electronic communication can be subject to criminal and civil liability. 18 U.S.C. § 2511(1), (4) & (5). But there are many exceptions to this general rule. The exception relevant to this interlocutory appeal of an order on a motion to dismiss is that it is

not unlawful "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*." *Id.* § 2511(2)(g)(i) (emphasis added).

If the "electronic communication" is a "radio communication," there is a statutory definition of "readily accessible to the general public." *Id.* § 2510(16). As most relevant here, a *radio* communication that is not "scrambled or encrypted" is, by statutory definition, readily accessible to the general public. *Id.* § 2510(16)(A). If the intercepted electronic communication is *not* a radio communication, however, the statute provides no express definition of "readily accessible to the general public."

The Court held (a) that an unencrypted Wi-Fi communication is *not* a radio communication, and (b) if treated as a *non*-radio electronic communication, an unencrypted Wi-Fi communication is *not* readily accessible to the general public.

B. The Court's ruling imperils standard practices in the information technology industry, and is based on incorrect factual assumptions about Wi-Fi technology.

The Court's ruling needlessly treats modern digital wireless communications in a manner that is fundamentally different than the treatment of old-world analog wireless communications. This deviation from technology neutrality puts standard practices used by the information technology ("IT") industry at legal risk. Most

notably, the ruling calls into legal question practices used by IT security professionals every day to secure wireless networks. As a result, the Court's decision will make it *harder* for IT security professionals to their jobs, thus rendering wireless networks *more* susceptible to intrusion. This cannot be what Congress intended.

Second, the Court's holding that an unencrypted Wi-Fi communication is *not* readily accessible to the general public, assuming it is *not* a radio communication, rests on faulty factual assumptions. The Court justified its conclusion on two grounds.

The Court's first basis for its holding is that an unencrypted Wi-Fi communication is not "readily" available because Wi-Fi networks typically have a limited geographic scope. But Wi-Fi networks do not have clear geographic bounds, and regularly reach into public areas that are, in fact, "readily" available to the general public. Indeed, the very communications at issue in this case were accessed from public streets.

The Court's second basis for its holding is that an unencrypted Wi-Fi communication is "encoded" and sent to a "specific destination"—and that as a result "sophisticated hardware and software" is needed to receive and decode the communication from another computer. But *encoding*—as distinct from *encryption*—does nothing to render a communication inaccessible. In fact, the Wi-

Fi specifications note that data passed over unencrypted wireless connections are "unprotected." Similarly, the fact that the encoding includes a destination address does nothing to render the communication *inaccessible* to another computer on the wireless network. Moreover, the hardware and software used for packet sniffing are no more sophisticated than the hardware and software used for all Wi-Fi communications. And, in fact, the televisions, set-top boxes and digital video recorders that the general public readily uses to access television broadcasts—which the Court held are not radio communications—are similarly sophisticated, and the broadcasts are also encoded, yet no one would dispute that unscrambled, unencrypted television broadcasts are readily accessible to the general public.

In short, neither of the Court's factual bases for its holding that an unencrypted Wi-Fi communication is not readily accessible to the general public is correct. ITIF urges the Court to grant rehearing or rehearing en banc.

III. ARGUMENT

A. The Court's interpretation would place at legal risk standard techniques used every day by information technology professionals at companies around the country.

IT professionals routinely engage in packet sniffing and subsequent packet analysis to do their jobs. In particular, IT security professionals use packet sniffing and analysis to comply with various security requirements in, for example, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act,

and the Sarbanes-Oxley Act. IT security professionals also use packet sniffing and analysis to ensure compliance with, for example, data security standards in the payment card industry such as Visa's Cardholder Information Security Program, and with standards required by the Department of Defense.

Packet sniffing and analysis are valuable, standard tools for IT professionals for a host of reasons:

Detecting unauthorized wireless network access points: IT security professionals can use packet sniffing and analysis to detect unauthorized wireless network access points that could allow attackers onto a corporate network or allow employees to circumvent network security controls.[2] To mitigate this risk, IT security professionals will actively scan for unauthorized access points. Actively scanning for unauthorized access points involves monitoring all wireless traffic to create a list of all access points in use.

Stopping "evil twin" or "WiFishing" attacks: IT security professionals also perform packet sniffing and analysis to detect rogue wireless network access points

[2] Because of the lack of security on an unencrypted Wi-Fi network, "the connection of a single wireless link (without data confidentiality) to an existing wired LAN may seriously degrade the security level of the wired LAN." IEEE Standards Association, *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* 75 (2012) (hereinafter "*Wireless Specifications*").

("evil twin" or "WiFishing" attacks). A rogue access point is one that broadcasts the Service Set Identifier ("SSID") of a legitimate access point so that users will inadvertently connect to the rogue network. To mitigate this risk, IT security professionals monitor wireless traffic to detect beacons from unauthorized access points.

Locating unauthorized Wi-Fi devices: IT security professionals can also use packet sniffing and analysis to detect unauthorized Wi-Fi devices. Some organizations prohibit employees from bringing unauthorized wireless devices to their facility. To detect a violation of this policy, organizations might monitor wireless traffic to track the addresses of Wi-Fi devices in operation.

Protecting against network intrusions: Capturing wireless traffic also allows IT security professionals to protect against attacks by detecting active scanning, a probing technique used by intruders to identify wireless networks. Similarly, IT security professionals can capture wireless traffic to analyze wireless packets for malicious or anomalous activities that indicate a potential threat. For example, wireless packet payload data can be analyzed to detect malware, such as computer viruses, or other attack signatures, such as denial of service attacks.

Optimizing network performance: Standard network management practices can also involve monitoring wireless traffic. For example, Wi-Fi networks operate in the 2.4 GHz spectrum. There are limited channels available for communicating

on a Wi-Fi network. To optimize performance, a home user or company might monitor wireless traffic to determine the optimal channel to use. Because the use of channels can change over time, such analysis might need to be repeated regularly to optimize network performance.

In all of the above cases, an IT professional might capture unencrypted Wi-Fi communications. In dense, urban settings, corporate Wi-Fi networks and home Wi-Fi networks frequently overlap. As a result, IT professionals performing their jobs might well capture packets not only from the corporate network, but also from other networks as well. In fact, without inspecting payload data, in many cases they will not be able to distinguish between activity on an overlapping non-corporate network, which presents no security concerns, and insecure or malicious traffic on the corporate network.

The Court's decision thus raises serious questions about the legality of these industry-standard techniques. It makes little sense to assume that Congress intended to render unlawful the receipt and decoding of an unencrypted Wi-Fi communication when Congress expressly stated the precisely opposite conclusion for an unencrypted and unscrambled "radio communication." *See* 18 U.S.C. § 2510(16). Instead, absent a clear expression to the contrary, the Court should assume that Congress did not intend to apply different rules to wireless

communications based on whether old-world analog or modern digital technologies are used.

B. The Court's conclusion that an unencrypted Wi-Fi communication is not readily accessible to the general public is incorrect as a matter of technological fact.

ITIF takes no position on the meaning of "radio communication" as a matter of statutory construction. Op. 13-31; Pet. 4-12. If a Wi-Fi communication is *not* radio communication—and if the statutory definition in 18 U.S.C. § 2510(16) therefore does not apply—ITIF likewise takes no position on whether it was properly before the Court to resolve the question of whether an unencrypted Wi-Fi communication is readily accessible to the general public. Pet. 12-15.

However, *if* a Wi-Fi communication is not a radio communication, and *if* the Court does reach the issue of whether an unencrypted Wi-Fi communication is readily accessible to the general public, ITIF urges the Court to reconsider its conclusion. As a matter of technological fact, an unencrypted Wi-Fi communication *is* readily accessible to the general public.

1. Wi-Fi communications are "readily" accessible to the general public regardless of the transmission range of the access point.

The Court concluded that because Wi-Fi access points typically have a limited range, Wi-Fi communications are not "readily" available. Op. 33. But by their very nature, "well-defined coverage areas" for wireless networks "simply do

not exist."[3] That is why such communications can and do travel "beyond the walls of the home or office where the access point is located." Op. 33. Moreover, a Wi-Fi access point can be mobile, which both means that a larger geographic area can be part of its coverage area over time, and that the coverage area might well include locations frequented by the general public, such as coffee shops and airports.[4] And here, the communications at issue were intercepted *from public streets*—streets that are readily accessible to the general public. Op. 4. Nothing in 18 U.S.C. § 2511(2)(g)(i) suggests that a communication must be readily accessible to the members of the public *in a broad geographic area*.

Under the Court's interpretation, the legality of an interception could turn on the strength of the transmission and other environmental factors such as interference. But the person *receiving* a communication—the person potentially subject to civil and criminal liability under the Wiretap Act—cannot easily determine the geographic scope of the transmission. It will often be difficult or even impossible to distinguish between a received signal that is weak but intelligible because it was transmitted at low power from nearby (in which case it is unlawful to intercept the communication under the Court's interpretation) or

[3] *Wireless Specifications*, *supra* n.2, at 49.

[4] *See, e.g.*, Wikipedia Foundation, *MiFi*, http://en.wikipedia.org/wiki/MiFi.

because it is transmitted at high power from very far away (in which case it might be lawful to intercept the communication).

2. The fact that an unencrypted Wi-Fi communication is "encoded" (but not encrypted) for a "specific destination" does not mean it is not readily accessible to the general public.

In a Wi-Fi network, "all [Wi-Fi nodes] and certain other RF devices in or near the [network] might be able to send, receive, and/or interfere with the [network] traffic."[5] As a result, a Wi-Fi-enabled computer "can receive [Wi-Fi] traffic that is within range and can transmit to any other [Wi-Fi node] within range."[6] It is precisely for this reason that the Wi-Fi standard "provides several cryptographic algorithms to protect data traffic" that can be used to secure an access point.[7]

It is true that unencrypted Wi-Fi communications are encoded. Op. 34. But this *encoding* is nothing more than an agreed upon set of standards that explain how the communication can be interpreted—standards that are *public* and followed by all Wi-Fi-compliant hardware and software.[8] If a Wi-Fi communication is not secured using available *encryption* algorithms, the *encoding* does nothing to secure the communication. To the contrary, "[i]f the data confidentiality service is not

---

[5] *Wireless Specifications, supra* n.2, at 75.

[6] *Id.*

[7] *Id.*

[8] *See generally Wireless Specifications, supra* n.2.

invoked"—if no encryption algorithm is used—"all frames are sent *unprotected*."[9] The mere fact of encoding thus does nothing to render the communication less accessible, just as this brief is no less accessible to the general public by virtue of the fact that it is "encoded" in English. Similarly, unscrambled, unencrypted television broadcast communications are, by any reasonable understanding, readily accessible to the general public,[10] notwithstanding that they are encoded using well-known standards.[11]

And it is also true that part of the encoding for a Wi-Fi communication indicates a destination address for the data. Op. 34. But that address merely identifies the intended recipient.[12] The destination address thus does nothing to render the data any less accessible, just as the spoken request, "Steve, can you pick

---

[9] *Id.* at 75 (emphasis added).

[10] If Court on rehearing adopts Google's position regarding "radio communication," then television broadcasts are radio communications, in which case the statutory definition of "readily accessible to the general public" in 18 U.S.C. § 2510(16) applies. But in that event, Wi-Fi communications are, likewise, radio communications to which 18 U.S.C. § 2510(16) applies.

[11] *See, e.g.*, Wikipedia Foundation, *NTSC*, http://en.wikipedia.org/wiki/NTSC (describing the National Television System Committee system used for analog "[t]elevision encoding" in the United States); Wikimedia Foundation, *Advanced Television Systems Committee standards*, http://en.wikipedia.org/wiki/Advanced_Television_Systems_Committee_standards (describing the digital television encoding standard used in the United States).

[12] *Wireless Specifications*, *supra* n.2, at 387-88 (discussing "address" fields in a "MAC frame").

up the phone," is accessible to anyone who hears it, whether that person is Steve or not.

The Court reasons, however, that because a Wi-Fi communication is encoded, and sent to a specific destination, it cannot be received and decoded by another absent use of "sophisticated hardware and software." Op. 34. First, the accessibility to the general public of an electronic communication cannot turn on the sophistication of the required hardware or software. Most of the general public cannot readily build a television or a television set-top box. But the general public *can* readily access unscrambled, unencrypted television broadcast communications using commonly available, off-the-shelf hardware and/or software, such as televisions, set-top boxes, and digital video recorders.

Similarly, members of the general public can (and do) readily access Wi-Fi communications using commonly available, off-the-shelf hardware and software—personal computers with Wi-Fi cards. And if a member of the general public wants to inspect Wi-Fi packets other than those addressed to or from the user's computer,[13] off-the-shelf software for that purpose, such as the "Wireshark" network protocol analyzer, is also readily accessible to the general public—indeed,

[13] As already discussed, practices standard in the IT industry regularly require such inspection. *See* Part III.A, *supra*.

for free.[14] Wireshark is "the world's foremost network protocol analyzer," "lets you see what's happening on your network at a microscopic level," and "is the de facto (and often de jure) standard across many industries and educational institutions."[15] The software includes a setting that allows the user to capture all packets on a network segment instead of limiting captured packets to those being sent to and from the user's computer.[16] Wireshark is compatible with standard hardware running Microsoft Windows, Apple Mac OS X, and many other operating systems.[17] And the software is no more "sophisticated" than the network protocol software that is included in those operating system—software that is used by the general public every day to access the Internet.[18]

---

[14] Wireshark Foundation, *Wireshark · Go Deep*, http://www.wireshark.org. The list of developers who have contributed code to Wireshark includes email addresses from, among other companies, Alcatel, Cisco, and NetApp. Wireshark Foundation, *Wireshark · About*, http://www.wireshark.org/about.html. The software has been named one of the most important open-source applications of all time by eWeek, and has also been highly praised by PC Magazine. *See id.*

[15] Wireshark Foundation, *Wireshark · About*, http://www.wireshark.org/about.html.

[16] *See* Wireshark Foundation, *4.6. The "Edit Interface Settings" dialog box*, http://www.wireshark.org/docs/wsug_html_chunked/ChCapEditInterfaceSettingsSection.html ("Capture packets in promiscuous mode" setting). In some circumstances, the user could also need to use an alternate network driver, but in many instances the standard network driver that is already installed on the computer will suffice.

[17] Wireshark Foundation, *Wireshark · About*, http://www.wireshark.org/about.html.

[18] The Court expressed concern about the effect of finding that an unencrypted Wi-Fi communication is readily accessible to the general public because software such as Wireshark can be downloaded from the Internet. Under this interpretation, the

* * *

In short, neither of the Court's justifications for concluding that an unencrypted Wi-Fi communication is not readily accessible to the general public is consistent with the actual technological facts about Wi-Fi networks. Unencrypted Wi-Fi networks by design are unprotected, and regularly are accessible to the general public, from public property. And the general public can readily access and decode an unencrypted Wi-Fi communication using nothing more than commonly available, off-the-shelf hardware and software—hardware and software that is no more sophisticated than televisions, set-top boxes and digital video recorders that the general public uses every day to access unscrambled and unencrypted television broadcasts.

Court reasoned that every computer keystroke would be accessible simply because hardware key loggers are easily purchased online. Op. 34 n.8. But it is not the sophistication of the hardware or software in a key logger that prevents computer keystrokes from being "readily accessible to the general public." Instead, keystrokes are not readily accessible to the general public because in order to capture them using a key logger, the device must be physically installed on a computer; the general public does not have ready physical access to others' computers.

IV. CONCLUSION

ITIF urges the Court to avoid unnecessarily adopting an interpretation of 18 U.S.C. § 2511(2)(g)(i) that treats modern digital wireless communications fundamentally differently than old-world analog wireless communications. Such a result would place standard IT practices at legal risk, and thus would *hamper* information security by restricting the means by which IT security professionals secure wireless networks. The Court's interpretation is unnecessary, because it is based on erroneous factual assumptions about Wi-Fi technology. Under the correct facts, an unencrypted Wi-Fi communication is readily accessible to the general public, even assuming it is not a "radio communication" within the meaning of the Wiretap Act.

DATED: October 4, 2013

/s/ Ashok Ramani

Ashok Ramani
Michael S. Kwun
Keker & Van Nest LLP
Counsel for Amicus Curiae
Information Technology & Innovation Foundation

CERTIFICATE OF COMPLIANCE

I certify, pursuant to Circuit Rule 29-2(c)(2), that this brief contains 3,427 words, excluding the parts exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 and 14 point Times New Roman.

/s/ Ashok Ramani
Ashok Ramani

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 4, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Roseann Cirelli
Roseann Cirelli

Case No. 11-17483

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BENJAMIN JOFFE, *et al.*,
Plaintiffs-Appellees,

v.

GOOGLE INC.,
Defendant-Appellant

On Appeal from the United States District Court
for the Northern District of California, Case No. 5:10-MD-2184-JW
Hon. James Ware, U.S. District Judge

CORPORATE DISCLOSURE STATEMENT OF AMICUS CURIAE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

ASHOK RAMANI
MICHAEL S. KWUN
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111-1809
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

Counsel for Amicus Curiae
Information Technology & Innovation
Foundation

October 4, 2013

Amicus Curiae Information Technology & Innovation Foundation has no parent corporation, and no publicly held corporation owns 10% or more of its shares.

DATED: October 4, 2013

/s/ Ashok Ramani

Ashok Ramani
Michael S. Kwun
Keker & Van Nest LLP
Counsel for Amicus Curiae
Information Technology & Innovation
Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 4, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Roseann Cirelli
Roseann Cirelli