Can We Sniff [Wi-Fi]? Implications of Joffe v. Google for security researchers and educators

Garfinkel, Simson L.
Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/44324
Can We Sniff [Wi-Fi]?
Implications of *Joffe v. Google* for security researchers and educators

Simson L. Garfinkel & Michael McCarrin
Naval Postgraduate School
Feb 18, 2014
http://simson.net/
NPS is the Naval Postgraduate School

Monterey, CA — 1500 students
  • US Military & Civilian (Scholarship for Service & SMART)
  • Foreign Military (30 countries)

Graduate Schools of Operational & Information Sciences (GSOIS)
  • Computer Science
  • Defense Analysis
  • Information Sciences
  • Operations Research
  • Cyber Academic Group

National Capital Region (NCR) Office
  • 900 N Glebe (Ballston)/Virginia Tech building
We analyze (“exploit”) information on modern computer systems.

- **MEDEX** — “Media” — Hard drives, camera cards, GPS devices.
- **CELEX** — Cell phone
- **DOCEX** — Documents
- **DOMEX** — Document & Media Exploitation

**Current Partners:**
- Law Enforcement (FBI & Local)
- DHS (HSARPA; Video Games & Insider Threat
- NSF (Courseware development)
- DOD
**Joffe v. Google** — A class-action lawsuit against Google for collecting unencrypted Wi-Fi traffic in the US.

Between 2007 and 2008 Google collected Wi-Fi data around the US (and overseas).

In 2010 several lawsuits were filed against Google for violating the Wiretap Act.

The Wiretap Act specifically states that it is “not unlawful” to intercept unencrypted radio communications that are “readily accessible to the general public.”

Google filed for dismissal, citing the Wiretap Act.
- The trial court refused.
- Google appealed.

On December 7th, 2013, the US Court of Appeals for the Nine Circuit issued an opinion:
- Data transmitted over a Wi-Fi network is not a “radio communication” under 18 USC § 20510(16).
  —*Therefore the Wiretap Act’s exemption may not apply.*
- Unencrypted Wi-Fi is not “publicly accessible.”
Many technologists are confused by this ruling.

Typical comment: “You mean, I can’t listen to radio waves passing through my own body?”

It depends...
Many technologists are confused by this ruling.

Typical comment: “You mean, I can’t listen to radio waves passing through my own body?”

It depends...
Many technologists are confused by this ruling.

Typical comment: “You mean, I can’t listen to radio waves passing through my own body?”

1980s unencrypted cordless phone

Legal to listen in

It depends...
Many technologists are confused by this ruling.

Typical comment: “You mean, I can’t listen to radio waves passing through my own body?”

It depends...
This talk explains the background and implications of the 9th Circuit Court’s recent decision in *Joffe v. Google*

**Background on Google Street View and Wi-Fi**

**More background on the ECPA and the Court’s decision**

**Implications for educators**
About Google StreetView and Wi-Fi
In 2007 Google launched Street View.

Street View is based on photos taken on the street.
Street View’s data come from this fancy camera.

http://www.google.com/maps/about/behind-the-scenes/streetview/
The camera takes many photos.

Collecting Imagery
First off we need to actually drive around and photograph the locations to show in Street View. We pay close attention to many factors, including the weather and and the population density of various areas, to determine when and where can collect the best possible imagery.

Aligning Imagery
To match each image to its geographic location on the map, we combine signals from sensors on the car that measure GPS, speed and direction. This helps us reconstruct the car’s exact route, and even tilt and realign images as needed.

Turning photos into 360-degree panoramas
To avoid gaps in the panoramas, adjacent cameras take slightly overlapping pictures, and then we "stitch" the photos together into a single 360-degree image. We then apply special image processing algorithms to lessen "seams" and create smooth transitions.

Showing you the right image
How quickly the car’s three lasers reflect off surfaces tells us how far a building or object is, and enables us to construct 3D models. When you move to an area in the distance, the 3D model determines the best panorama to show you for that location.
The photos are aligned and “stitched” together.

Collecting Imagery
First, we need to actually drive around and photograph the locations to show in Street View. We pay close attention to many factors, including the weather and the population density of various areas, to determine when and where can collect the best possible imagery.

Aligning imagery
To match each image to its geographic location on the map, we combine signals from sensors on the car that measure GPS, speed and direction. This helps us reconstruct the car’s exact route, and even tilt and realign images as needed.

Turning photos into 360-degree panoramas
To avoid gaps in the panoramas, adjacent cameras take slightly overlapping pictures, and then we "stitch" the photos together into a single 360-degree image. We then apply special image processing algorithms to lessen "seams" and create smooth transitions.

Showing you the right image
How quickly the car’s three lasers reflect off surfaces tells us how far a building or object is, and enables us to construct 3D models. When you move to an area in the distance, the 3D model determines the best panorama to show you for that location.
A “Neural Network” identifies house numbers.

“Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks,” Goodfellow, Bulatov, Ibarz, Arnoud and Shet, January 1, 2014
http://arxiv.org/abs/1312.6082

Technology Review.com
January 6, 2014
LIDAR provides 3D data for building outlines and setbacks.
Today Street View is available in many countries.
Part of Google’s plan for "Global Domination."

Google’s Road Map to Global Domination

Luc Vincent, the man in charge of all the imagery in Google's online maps, next to a Trekker.

By Adam Fisher
Published: December 11, 2013

Fifty-five miles and three days down the Colorado River from the put-in at Lee's Ferry, near the Utah-Arizona border, the two rafts in our little flotilla suddenly encountered a storm. It sneaked up from behind, preceded by only a cool breeze. With the canyon walls squeezing the sky to a ribbon of blue, we didn't see the thunderhead until it was nearly on top of us.
Street View’s cars are also equipped with Wi-Fi receivers.

Every Wi-Fi radio has a 48-bit “MAC Address”
• Assigned by manufacturer.
• Changeable, but rarely changed.

—Any Wi-Fi radio can be configured as an “Access Point,” a “Station” or other modes.
Wi-Fi is a primary means for access the Internet today.

Wi-Fi — 802.11 networking
- Ubiquitous — Laptops, Cell phones, Home Routers
- Coffee shops, Universities, Homes
- A primary means for accessing Internet

Wi-Fi Statistics (www.factbrowser.com/tags/wifi)
- 2011 increase in $ sales of wireless APs: 31%
  increase in $ sales of wired APs: 6%
- 2012: 75% of smartphone owners use WiFi
- 2012: 63% of U.S. adults use wireless Internet
- 2012: All 840 Macy’s and Bloomingdale’s stores provide Wi-Fi
- 2013: 86% of tablets require a wifi to access Internet

Everybody in this room probably uses Wi-Fi.
(But hopefully not right now.)

http://www.flickr.com/photos/superamit/45934256
Wi-Fi uses radio waves.
Radio waves move in all directions.

Wi-Fi Sniffing:
passive interception of Wi-Fi signals by a third party

http://www.flickr.com/photos/orinrobertjohn/902282459
“Beacons” are a kind of management frame. Each beacon contains:

- MAC and SSID (Service Set Identifier)
- Encryption Status

Wi-Fi Access Points send three kinds of packets: Control Frames, Management Frames, & Data Frames.
Google’s cars recorded Wi-Fi beacons & GPS coordinates.

Wi-Fi “Access Point”

Wi-Fi “Station”

60:03:08:9a:6a:10

BEACON
ishmael
72:00:01:80:40:f0

40.6083, -74.1533

BEACON
linksys
72:00:01:80:40:f0

40.6083, -74.0534

BEACON
archy
78:10:11:12:11:11

40.6123, -74.1542
Many houses have Wi-Fi. Each device in every house has a different MAC address.

Street View car in New Jersey
http://www.flickr.com/photos/njtechteacher/8188781999
Wi-Fi Access points rarely move. Recording their location lets Google use Wi-Fi like GPS. This is especially useful indoors & in cities. Skyhook Wireless patented the basic idea in 2003.
In 2010 German privacy regulators forced a review of the StreetView program. Google discovered that it was also capturing data frames.

April 27, 2010 — Google announces “Data collected by Google Cars”

May 17, 2010 — Google announces that Irish Data Protection Authority asked Google to delete “payload data we collected in error in Ireland”
Google hired Stroz Friedberg to analyze its software.

Stroz Friedberg’s report “confirms that Google did indeed collect and store payload data from unencrypted Wifi networks, but not from networks that were encrypted.”

- Technology stack:

Google’s software:
- parsed control frames
- archived and ignored unencrypted data frames.
The FCC conducted its own investigation.

November 3, 2010

• FCC sends a Letter of Inquiry (LOI) to Google requesting additional information.
• Potential violation of Section 705(a) of the Communications Act.
• FCC was concerned about the collection of “payload data.”

FCC Interviewed five Google engineers and an employee of Stroz Friedberg:

• “Engineer Doe invoked his Fifth Amendment right against self-incrimination and refused to testify.”
• “For many months, Google deliberately impeded and delayed the Bureau’s investigation by failing to respond to requests for material information...”
• “Although a world leader in digital search capability, Google took the position that searching its employees’ e-mail ‘would be a time-consuming and burdensome task.’ ”
FCC’s conclusion: lots of data were collected.

“Between May 2007 and May 2010, as part of its Street View Project, Google Inc. collected data from Wi-Fi networks throughout the United States and around the world.”

— Federal Communications Commission, April 2012

Conclusion: 600GB of unencrypted data captured in 30 countries

- Names
- Addresses
- Telephone numbers
- URLs
- passwords
- e-mail
- text messages
- medical records
- video
- audio

600GB ≈ 1 hard drive
FCC fined Google $25,000 — but not for potential violations.

“[W]e find that Google, which holds Commission licenses, is apparently liable for a forfeiture penalty of $25,000 for its noncompliance with Bureau information document requests.”

FCC chose not to enforce the potential violation of 705(a).
- There was no history of finding Wi-Fi sniffing a Wiretap Act violation.
Several class-lawsuits were filed against Google. Consolidated in *Joffe v. Google (5:10-md-02184-JW)*

August 17, 2010
• Transferred to CA Northern District.

December 17, 2010
• Google files **Motion to Dismiss**
Google’s motion to dismiss is based on the Wiretap Act.

The “Wiretap Act” — 18 USC § 2511 and 18 USC § 2510 (Definitions)
- Prohibits interception of some kinds of communications by wire and radio.
- Significantly amended in 1986 by the Electronic Communications Privacy Act.
- Requires law enforcement to obtain warrants for interception in some cases.

The Wiretap Act generally allows interception of:
- Unencrypted “radio communications.”
- “Electronic communications” that are “readily accessible to the general public.”

“Radio communications” and “electronic communications” are not interchangeable.
- some of the definitions don’t quite make sense.
- This may be a drafting error — but it is the intent of Congress circa 1986.
The law:

18 USC § 2511 (2)
(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—
(i) 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 USC § 2510 (16)
“readily accessible to the general public” means, with respect to a radio communication, that such communication is not—
(A) scrambled or encrypted;
(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
(C) carried on a subcarrier or other signal subsidiary to a radio transmission;
(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

c.f. https://ilt.eff.org/index.php/Privacy:_Wiretap_Act
The trial court did not accept Google’s motion. Google appealed.

August 17, 2010
• Transferred to CA Northern District.

December 17, 2010
• Google files Motion to Dismiss

June 29, 2011
• ORDER granting in part and denying in part Motion to Dismiss

July 8, 2011
• Motion for a Certificate of Appealability

July 18, 2011
• Order granting Certificate of Appealability.
Google appealed the partial denial of its motion to dismiss to the US Courts for the Ninth Circuit.
The 9th Circuit denied Google’s appeal.

September 10, 2013
• Unencrypted Wi-Fi is not a “radio communication”
• Even if it is radio communication, it is not “readily accessible to the general public.”

September 24, 2013
• Google petitioned for Rehearing and for Rehearing En Banc

December 27, 2013
• Granted Rehearing, Denied Rehearing En Banc
• Issued revised opinion
• Unencrypted Wi-Fi is not a “radio communication”
• Even if it is radio communication, it is not “readily accessible to the general public.”

The Wiretap Act

A bit more background on the law

http://en.wikipedia.org/wiki/Macintosh_Plus
The 1986 Electronic Communications Privacy Act was drafted in part to protect cell phone communications.

1983 — Motorola’s Dynatax 800x is receives FCC approval.
- AMPS — Advanced Mobile Phone System
- 850 MHz in US
- Analog
- No encryption
  - Monitoring by scanners
  - Phone cloning (1990s)

1986 — Congress passes ECPA
- Made it illegal to listen to cell phone communications
- Scanners could be easily modified to eavesdrop on cell phone calls.
- Addressed “hobbyists’ concerns” to make it clear that “intercepting traditional radio services is not unlawful.” (Cong. Rec S7987-04)
Despite being illegal, many people listened …
ECPA criminalized cell phone eavesdropping, but not cordless phone eavesdropping.

1990 Tyler v. Berodt, 8th Circuit ruled that the Wiretap Act did not apply to cordless telephones.

- No “reasonable expectation” of privacy — people routinely heard each other’s calls on cordless phones.
1990: US Supreme Court declines to hear the Tyler v. Berodt cordless phone case on appeal.

No split among the lower courts, and “the fact that Congress amended the Wiretap Act to explicitly exclude cordless telephones means that cases of this nature will not arise under the Wiretap Act in the future.”

—Harray A. Blackmun’s scanned papers.
What about wireless data?

The purpose of the Wiretap Act:
—“To protect against unauthorized interception of electronic communications.”

The Wiretap Act uses several terms in slightly different contexts:
• “Electronic Communications”
• “Radio Communication”
• “Communication by Radio”

The Wiretap Act has a complex legislative history:
• Last major amendment in 1986 (Electronic Communications Privacy Act)
• 1990 — Senator Patrick Leahy’s task force to study wireless data
• 1994 — Congress added § 2510(16)(F) to protect wireless data
• 1996 — Congress repealed § 2510(16)(F)
—This history is discussed in the court’s opinion
The 9th Circuit December 27, 2013 ruling found that Wi-Fi is not a “radio communication.”

The Wiretap Act’s clear language allows the interception of:

- **Electronic communications** that are **readily accessible by the general public**

Where:

- “**readily accessible**” means **radio communications** that are **not encrypted**.

The 9th Circuit concluded that Wi-Fi is not “radio communication.”

—*Communication by radio is not necessarily “radio communication.”*

—“**The ordinary meaning of ‘radio communication’ does not include data transmitted over a Wi-Fi network**” (p. 13)

—“**Google’s proposed definition is in tension with how Congress—and virtually everyone else—uses the phrase… In common parlance, watching a television show does not entail ‘radio communication.’ Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network.**” (p. 15)
9th Circuit’s Hypothetical:
What if the police were running an unencrypted Wi-Fi?

“It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity.” (p. 15)
The 9th Circuit doesn’t consider penetration testing...

“Traditional radio services can be easily and mistakenly intercepted by hobbyists…

“But ‘radio hobbyists’ do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks.

“Lending ‘radio communications’ a broad definition that encompasses data transmitted on Wi-Fi networks would obliterate Congress's compromise and create absurd applications for the exemption for intercepting unencrypted radio communications.” (p. 22)

You are totally correct 9th Circuit!

Penetration testers and security enthusiasts intentionally use packet sniffers to intercept payload data transmitted over Wi-Fi networks.
Other courts have ruled differently

Federal District court in Illinois, *In re Innovatio IP Ventures, LLC.*

—“Because data packets sent over unencrypted Wi-Fi networks are readily accessible using the basic equipment described above, the Wiretap Act does not apply here.”
—October 3, 2013.

Note: This is a **district court** ruling, not an appellate court.

But — Wi-Fi sniffing will probably make its way to the Supreme Court.
How should Wi-Fi fit into the Wiretap Act?

We think of packets as traveling from the AP to the station, but that’s not accurate:

-X

Packets actually travel in spherical shells in all directions:

—So it’s easy for another party to intercept them.
Wi-Fi capture software is widely available.

MacOS:
Apple’s Sniffer can target any channel
There are many programs for analyzing sniffed data

Wireshark and EtherPeek look at *packets*

GUI-based tools can reconstruct entire web pages:

- OmniPeek
- Wireshark
- NetworkMiner
- NetIntercept
We can’t prevent packets from being intercepted. We use encryption to make the unintelligible.

Wireless encryption:
- WPA (Wi-Fi Protect Access)

Packet level encryption:
- VPN (e.g. Cisco VPN)

Application Layer:
- SSL/TLS (e.g. https:, SMTPS, IMAPS)

Document Layer:
- S/MIME & PGP (email)
- PDF encryption
- Microsoft Document encryption

Google enabled TLS for GMail when the Wi-Fi capture was discovered.
Implications for Education, Research and Technology

A bit more background

http://www.flickr.com/photos/jpellgen/3372418845
So what should we do for now?

Teaching:
• Set up a test network on a specific channel.
• Add filters to the capture — only capture your own MAC addresses.
• Don’t tell students to sniff in the wild!

Security practitioners:
• Be careful about Wi-Fi surveys
• Don’t sniff at Starbucks

Wireless users in general:
• Increasingly the web is going to be TLS-encrypted
• Strong prohibitions on sniffing will make wireless less secure
  —Most of the vulnerabilities were found by unauthorized sniffing
What is the right public policy?

Should it be legal to intercept their packets:
What is the right public policy?

Should it be legal to intercept their packets:

If it was 1988 and these people had wireless phones in the coffee shop...

Legal to sniff

Illegal to sniff
What is the right public policy?

Should it be legal to intercept their packets:

If it was 1988 and these people had wireless phones in the coffee shop...

Legal to sniff
unlicensed

Illegal to sniff
licensed
What is the right public policy?

Should it be legal to intercept their packets:

If it was 1988 and these people had wireless phones in the coffee shop...

Legal to sniff unlicensed

Illegal to sniff licensed

Unlike cell phones:
1. Wi-Fi beacons are designed to be intercepted by all stations.
2. Every station is a sniffer.
If sniffing is illegal, future security researchers may not aggressively look for vulnerabilities...

You can’t set up a highway network in a lab.
Is sniffing legal?

For now — try to avoid sniffing in the 9th Circuit.

Provider “terms of service” are likely to be important:
• AT&T WiFi prohibits operating a sniffer.
• Google WiFi is silent on the matter.

A future ruling is likely to depend upon:
• The protocol being sniffed. (Wi-Fi, Bluetooth, ZigBee, RFID)
• Whether the sniffed frequency is licensed or unlicensed.
• The use of encryption and cracking
• Whether the sniffed frames are beacons or content
• Whether the entire packet content is kept, or just the headers.

```bash
# tcpdump -i en0 -s 4096 -w full-content.pcap
```
References

“Source Code Analysis of gstumbler”, Stroz Friedberg, June 3, 2011

“Notice of Apparent Liability for Forfeiture,” FCC DA 12-592, April 13, 2012
—http://www.wired.com/images_blogs/threatlevel/2012/05/unredactedfccgoog.pdf (less redacted)

In re Innovatio IP Ventures, LLC Patent Litigation, 886 F.Supp.2d 888
—http://scholar.google.com/scholar_case?case=16680089225036893693

Joffe v. Google, 11-17483, US Courts for the 9th Circuit,

WiFi data collection: An update, Google, May 2010

Data Engineer in Google Case Is Identified, New York Times, April 30, 2012
—http://www.nytimes.com/2012/05/01/technology/engineer-in-gogles-street-view-is-identified.html