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

Simson L. Garfinkel & Michael McCarrin
Naval Postgraduate School

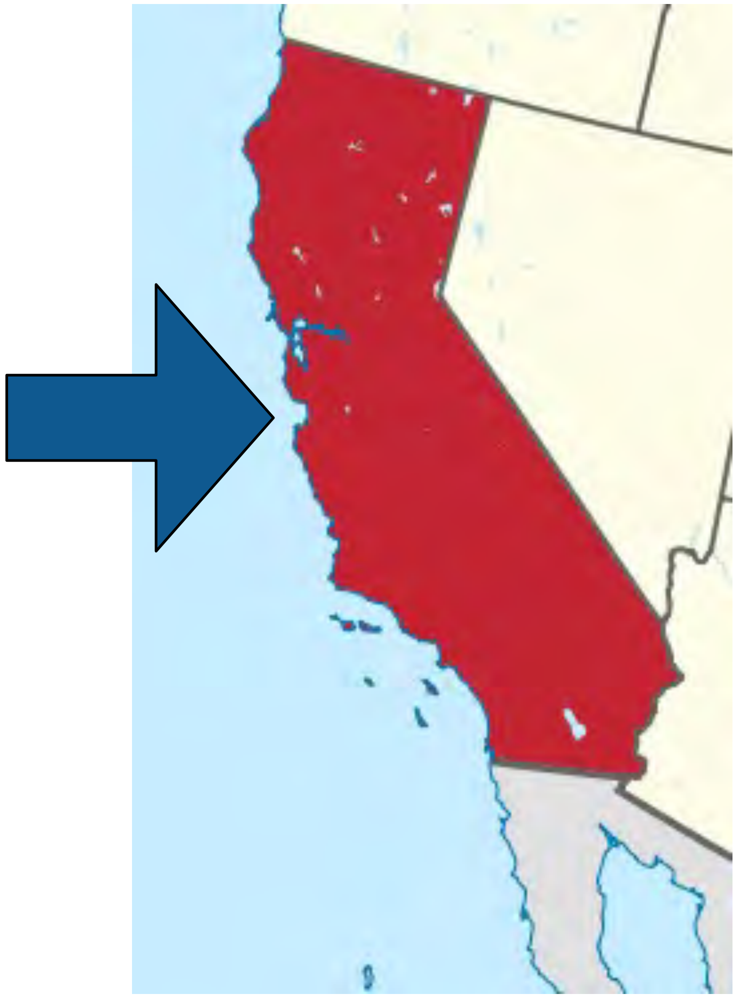
Feb 18, 2014

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

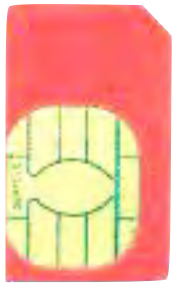
Digital Evaluation and Exploitation (DEEP): Research in “trusted” systems and exploitation.

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.”~~

Removed from revised opinion

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...

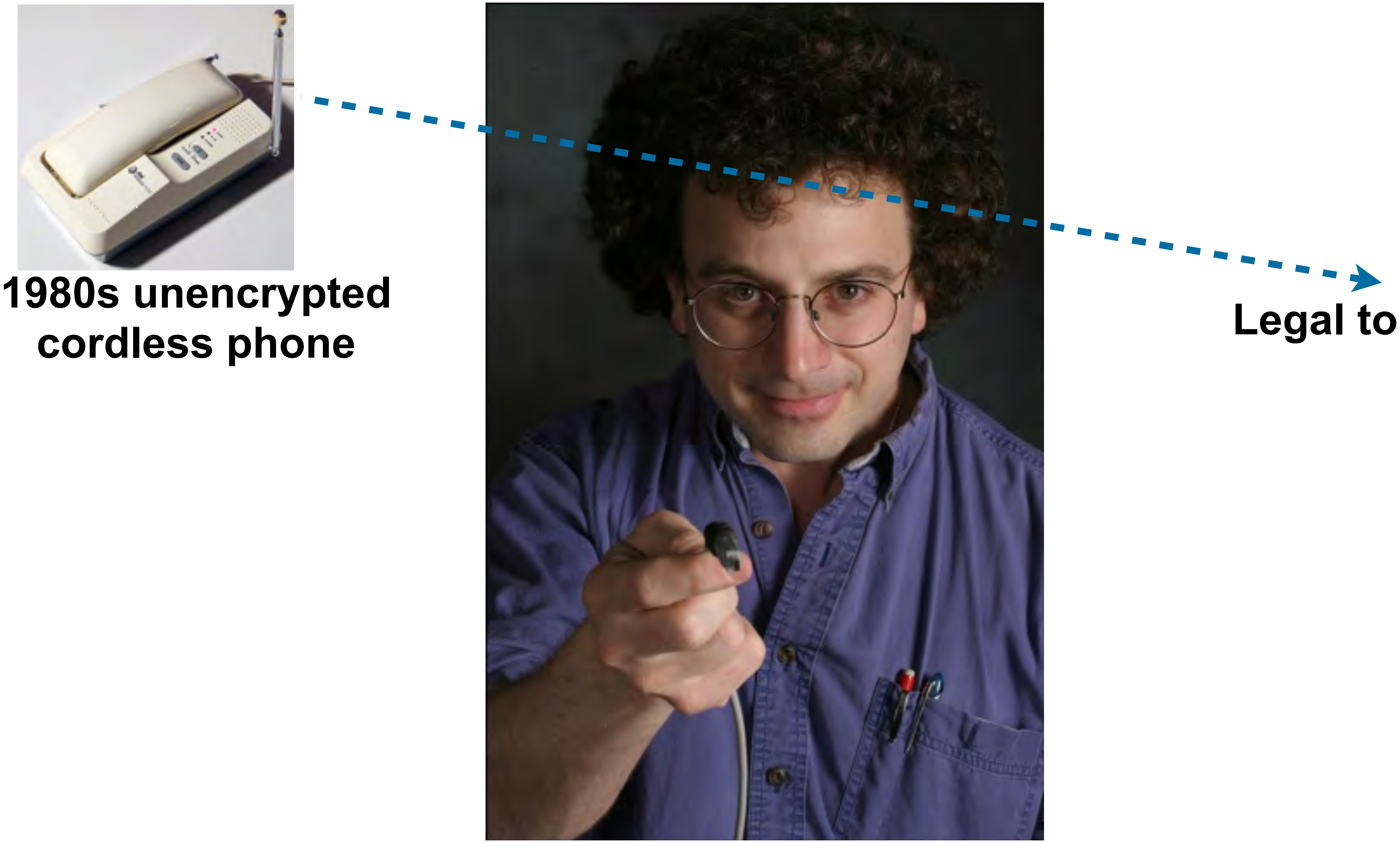
Many technologists are confused by this ruling.

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?”

1980s unencrypted cordless phone

1980s unencrypted cell phone

Legal to listen in

Illegal to listen in

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

http://www.flickr.com/photos/signlanguageltd/4626612028

About Google StreetView and Wi-Fi

In 2007 Google launched Street View.

Street View is based on photos taken *on the street*.

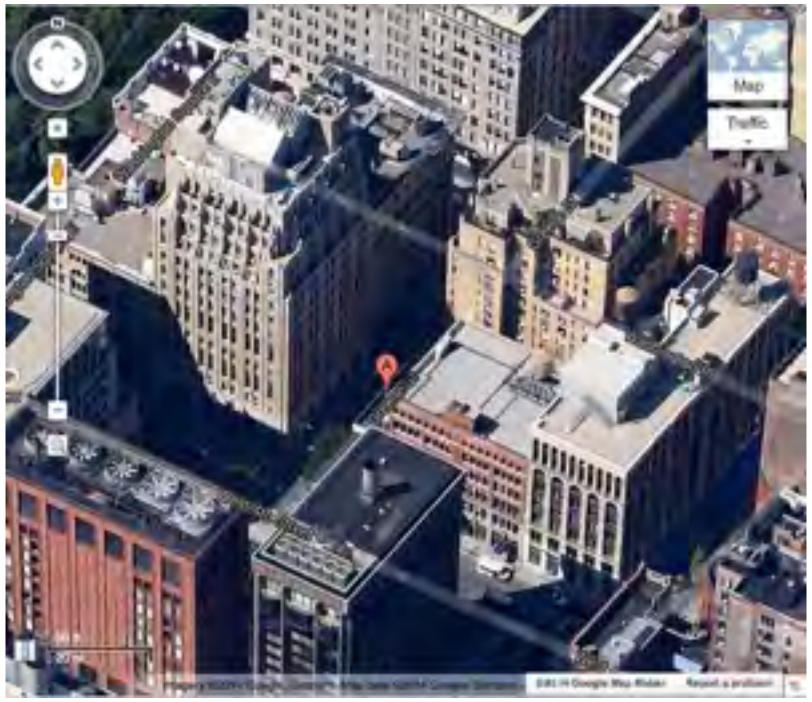
Map

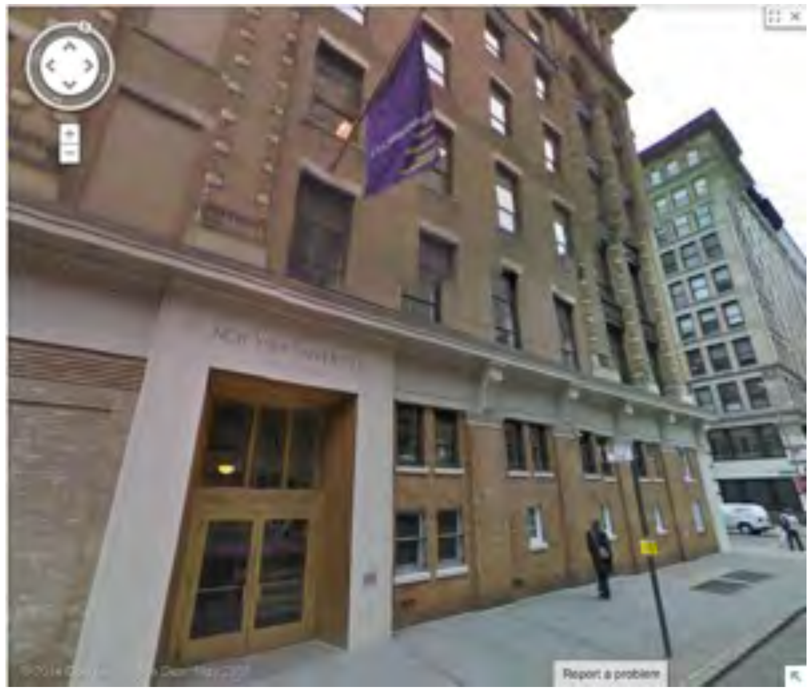
Satellite
Traffic
Washington Square Park
Washington Square E
West 4th Street
Washington Pl
Mercer St
Waverly Pl
Broadway
W 3rd St
Lafayette St
Great Jones St
Bleecker St
Courant Institute of Mathematical Sciences
Tisch School of Arts
CITIBANK N.A.
Starbucks
200 ft
100 m
Map data ©2014 Google, Sanborn
Edit in Google Map Maker
Report a problem

Map
Traffic
Edit in Google Map Maker
Report a problem

"Satellite"

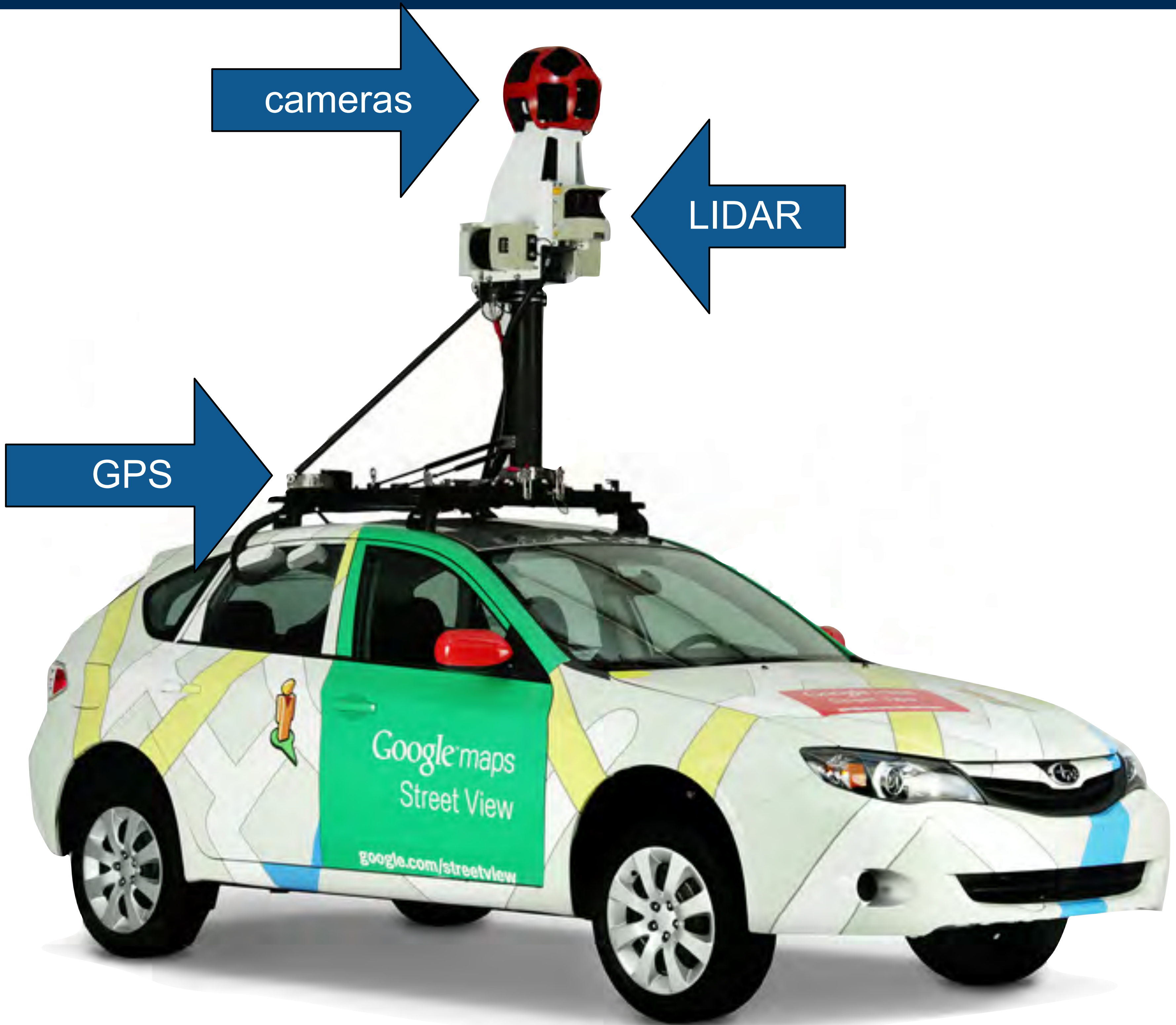
Aerial





Street View

Street View's data come from this fancy camera.



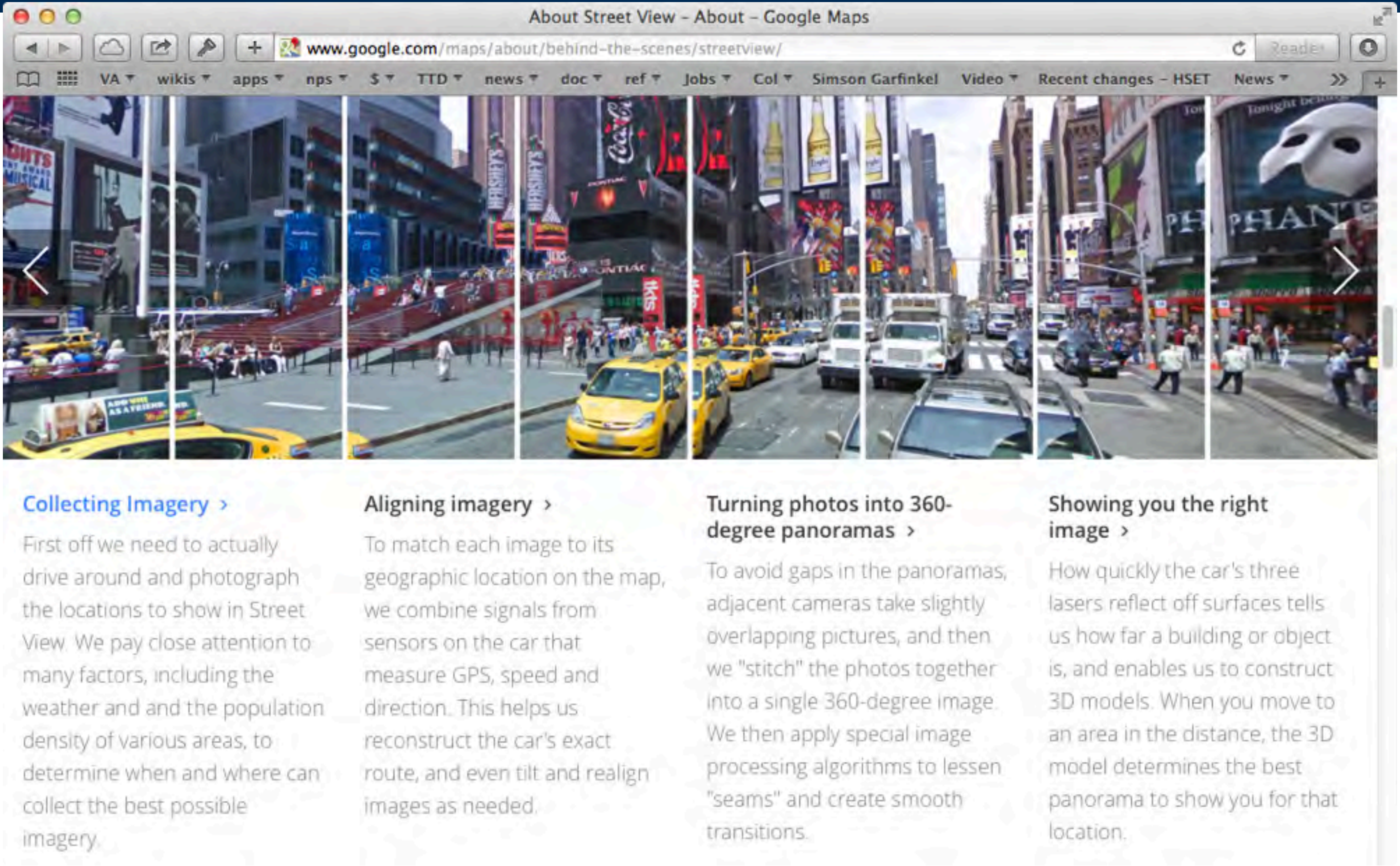
cameras

LIDAR

GPS

http://www.google.com/maps/about/behind-the-scenes/streetview/

The camera takes many photos.



About Street View - About - Google Maps
www.google.com/maps/about/behind-the-scenes/streetview/
Reader
VA
wikis
apps
nps
$
TTD
news
doc
ref
Jobs
Col
Simson Garfinkel
Video
Recent changes - HSET
News

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.

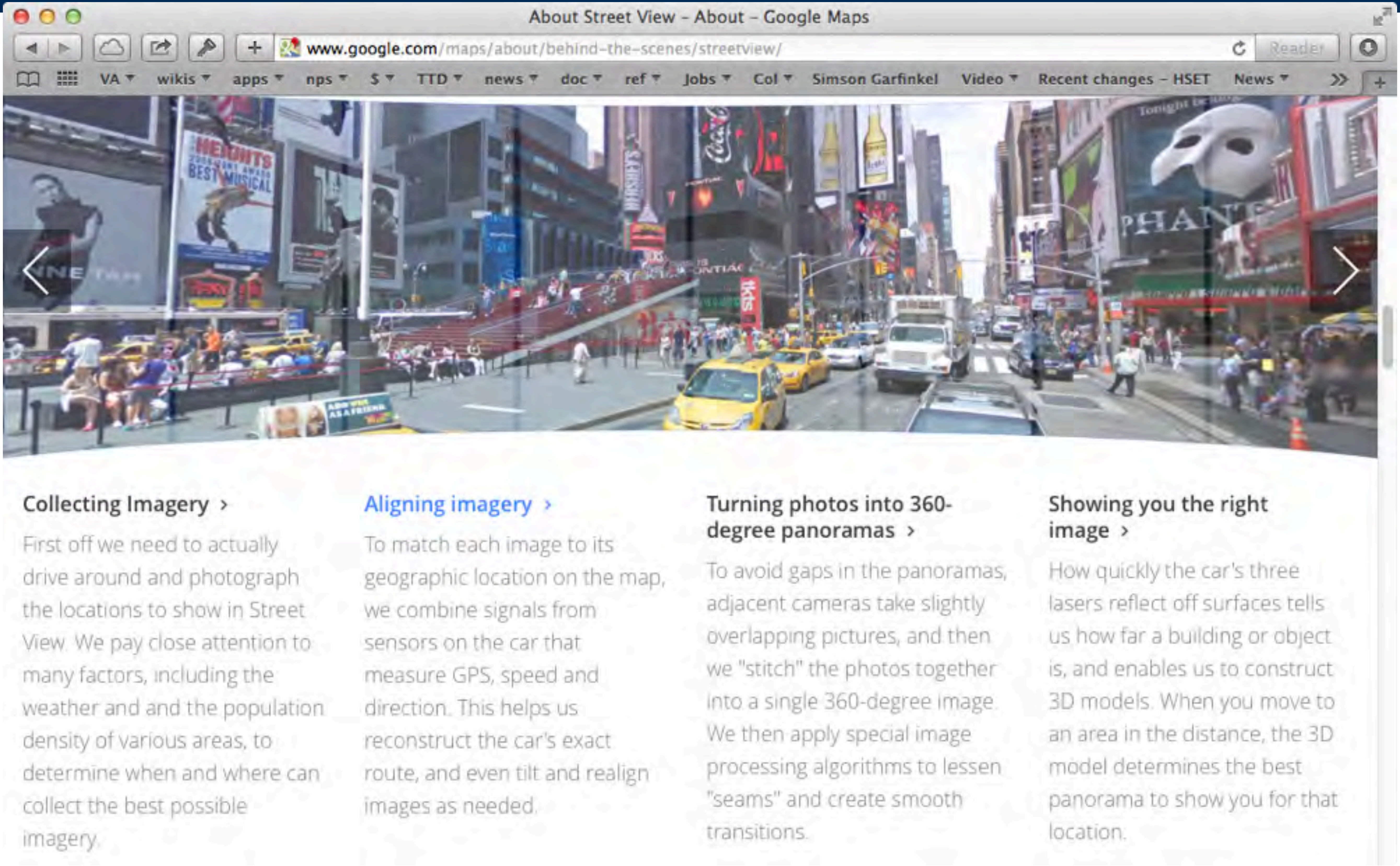
Turning photos into 360-degree panoramas ›

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.


About Street View - About - Google Maps
www.google.com/maps/about/behind-the-scenes/streetview/
Reader
VA
wikis
apps
nps
$
TTD
news
doc
ref
Jobs
CoI
Simson Garfinkel
Video
Recent changes - HSET
News

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.

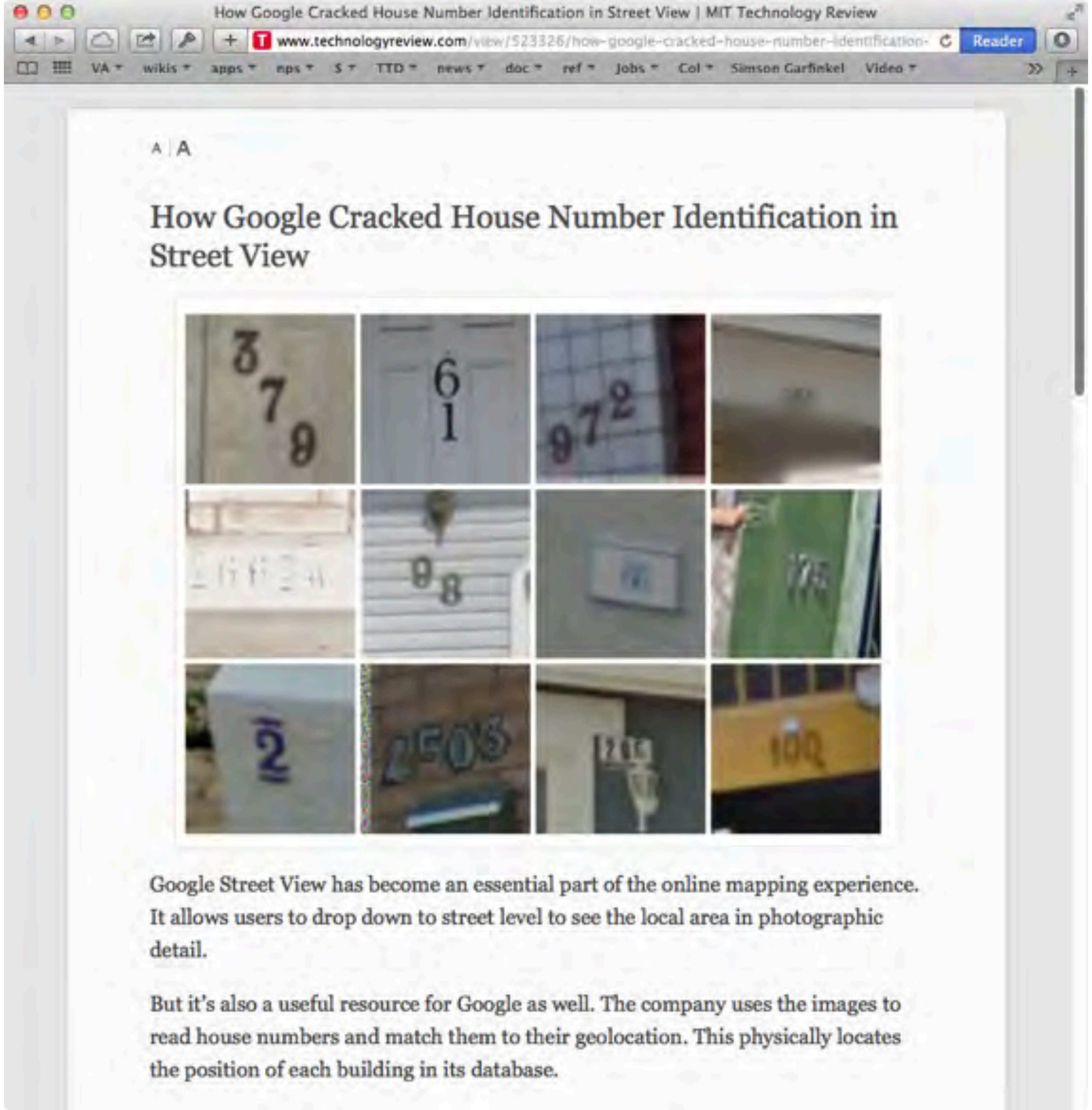
Showing you the right image ›

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.

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


How Google Cracked House Number Identification in Street View | MIT Technology Review
www.technologyreview.com/view/523326/how-google-cracked-house-number-identification-
Reader
VA
wikis
apps
nps
$
TTD
news
doc
ref
Jobs
Col
Simson Garfinkel
Video
A A

How Google Cracked House Number Identification in Street View

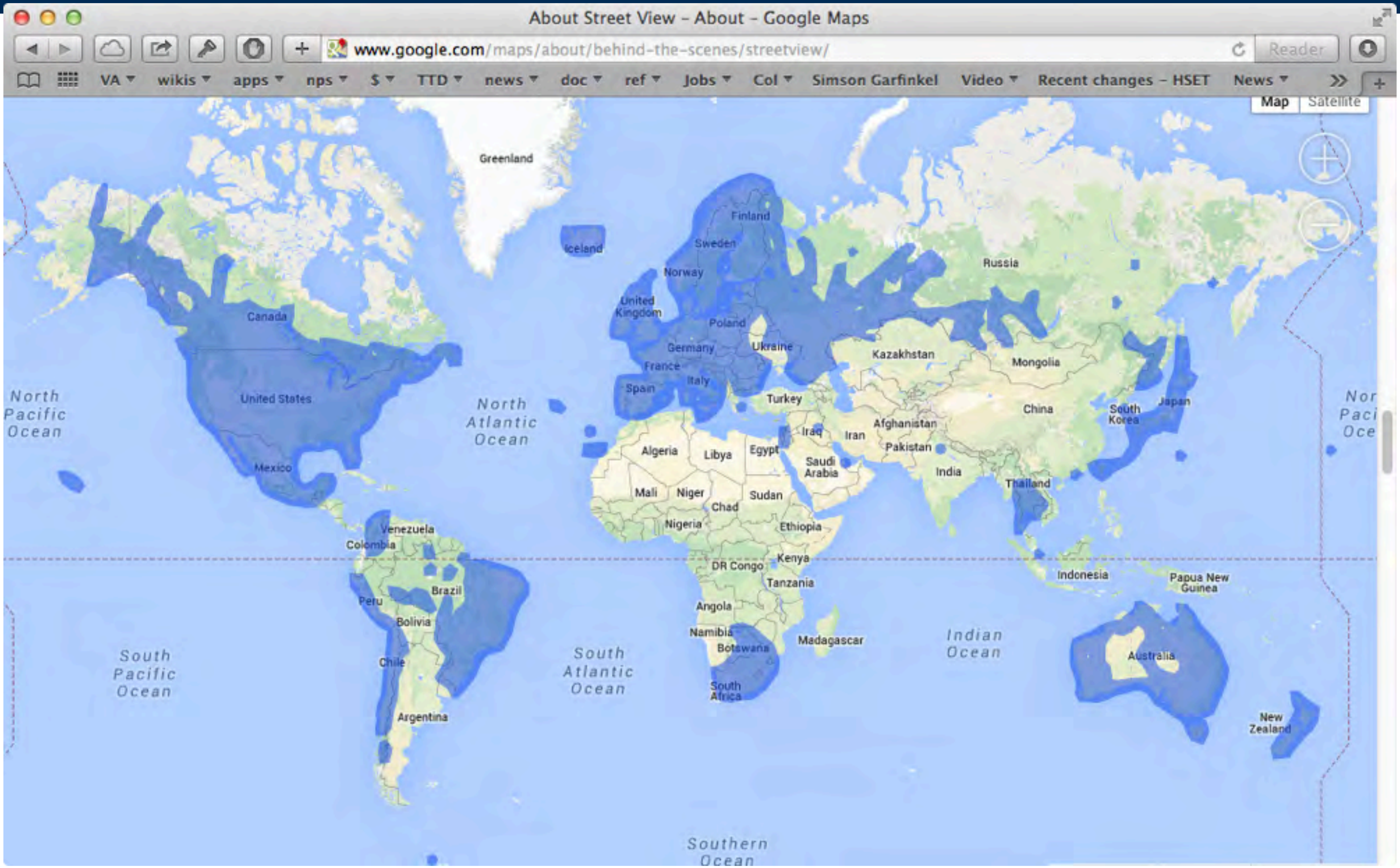
Google Street View has become an essential part of the online mapping experience. It allows users to drop down to street level to see the local area in photographic detail.

But it’s also a useful resource for Google as well. The company uses the images to read house numbers and match them to their geolocation. This physically locates the position of each building in its database.

LIDAR provides 3D data for building outlines and setbacks.

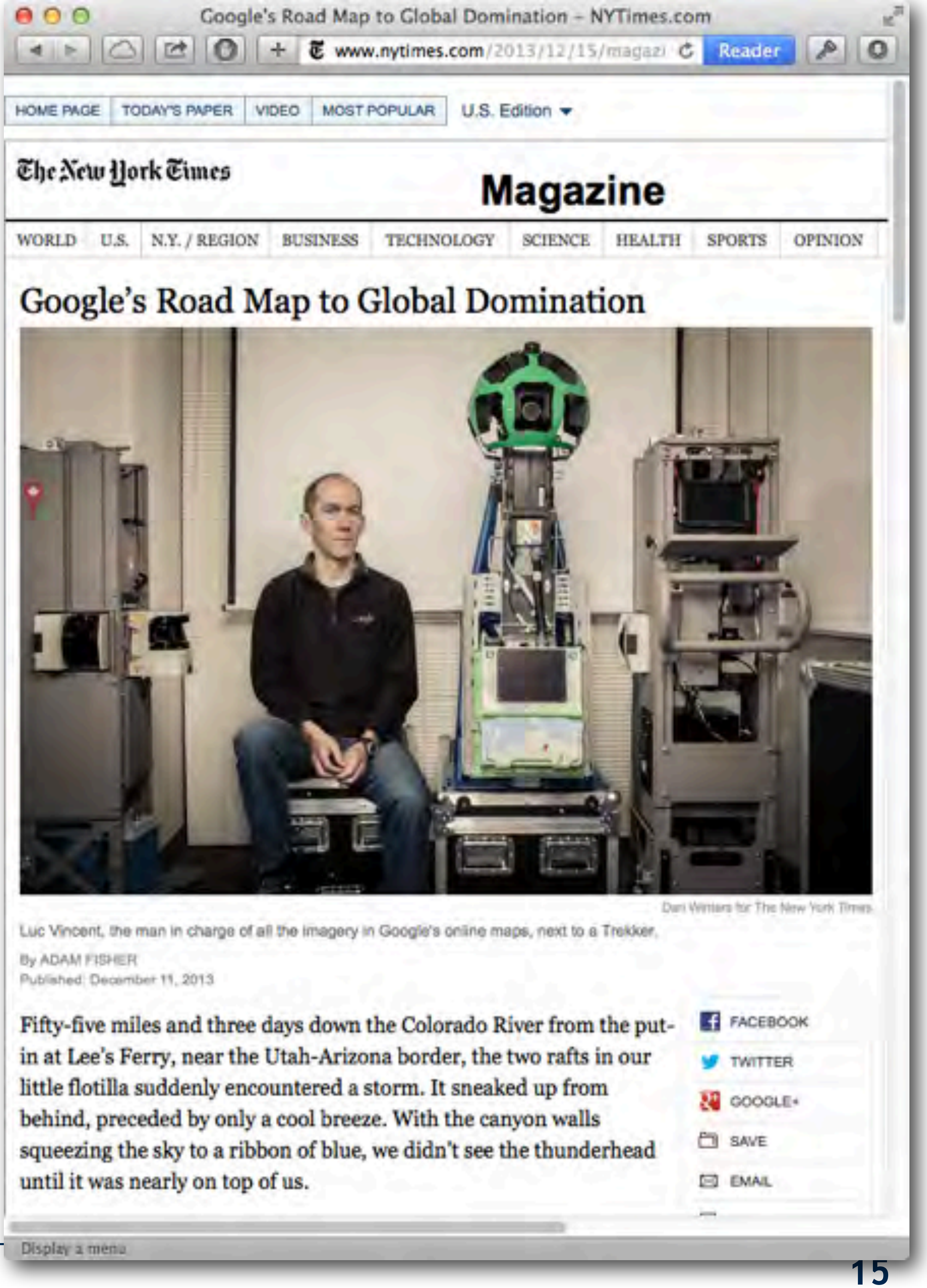
Room
Satellite
Traffic
Ellen M. Carroll, PNP
Washington Square E
Black Box Theatre
Nordoff-Robbins Music Therapy Foundation
NYU Pless Hall
Washington Pl
NYU
Goddard Residence Hall
Public Safety - Administrative Office
Starbucks
NYU
Washington Pl
New York University Postdoctoral Program in Psychotherapy & Psychoanalysis
Greene St
Schwartz Plaza
New York University: Dept of Linguistics
Washington
NYU Administrative & General
Babette
Campus Eatery
West 4th Street
NYU Stern School of Business
Gould Plaza
Kaufman Management Center
NYU Stern Executive MBA program
Econ NYU
West 4th Street
Zvi M. Kedem, NYU
NYU Stern School: Dept of Management & Organizations
COURANT LIBRARY
W 3rd St
Courant Institute of Mathematical Sciences
Bond New York Real Estate
Rolf Schewe - Licensed Real Estate Salesperson
Duane Reade Store New York
Think Coffee
50 ft
20 m
Constance Carr-Shepherd
W 3rd St
Map data ©2014 Google, Sanborn
Edit in Google Map Maker
Report a problem

Today Street View is available in many countries.



Part of Google's plan for "Global Domination."
— New York Times, Dec. 15, 2013

The New York Times Magazine
A FEAST OF BEASTS
BY SAM SIFTON
Google Was Here
IN THE BATTLE FOR DIGITAL DOMINANCE, VICTORY GOES TO THE ONE WHO CONTROLS THE MAP.
BY ADAM FISHER



Google's Road Map to Global Domination

Dan Winters for The New York Times

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

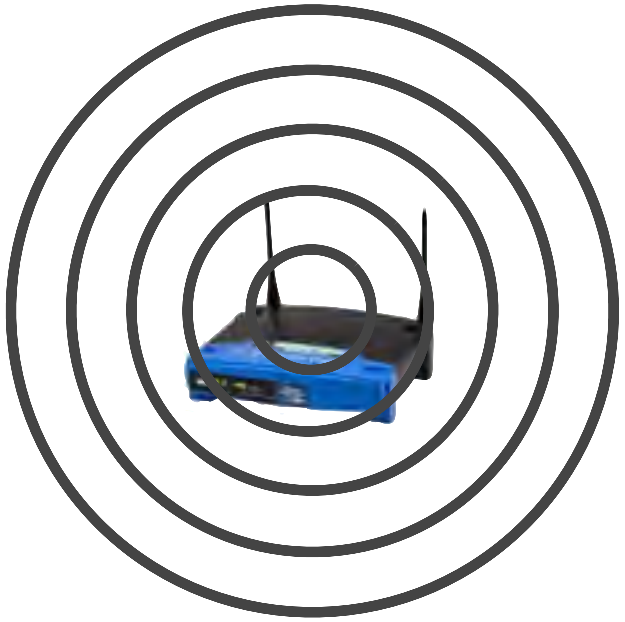
Fifty-five miles and three days down the Colorado River from the put-in at Lee's Ferry, near the Utah-Arizona border, the two rafts in our little flotilla suddenly encountered a storm. It sneaked up from behind, preceded by only a cool breeze. With the canyon walls squeezing the sky to a ribbon of blue, 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.

Wi-Fi "Access Point"



72:00:01:80:40:f0

Wi-Fi "Station"

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

—Any Wi-Fi radio can be configured as an "Access Point," a "Station" or other modes.

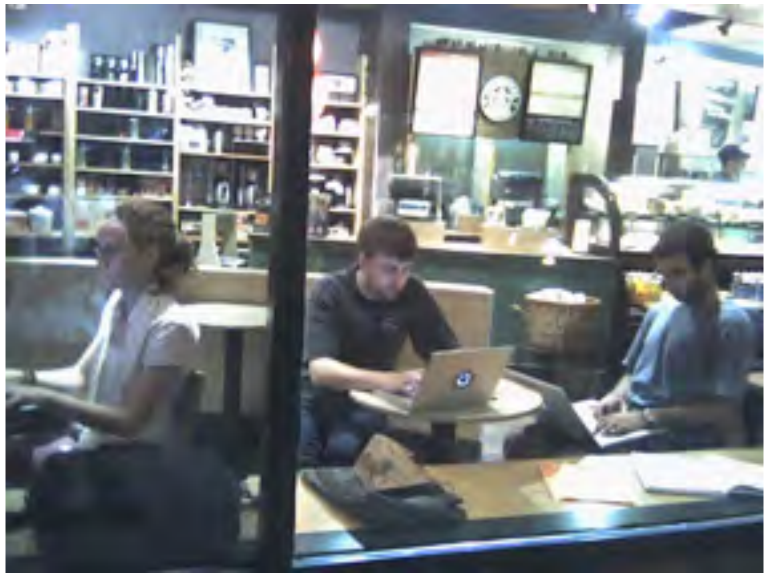
Wi-Fi is a primary means for access the Internet today.

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

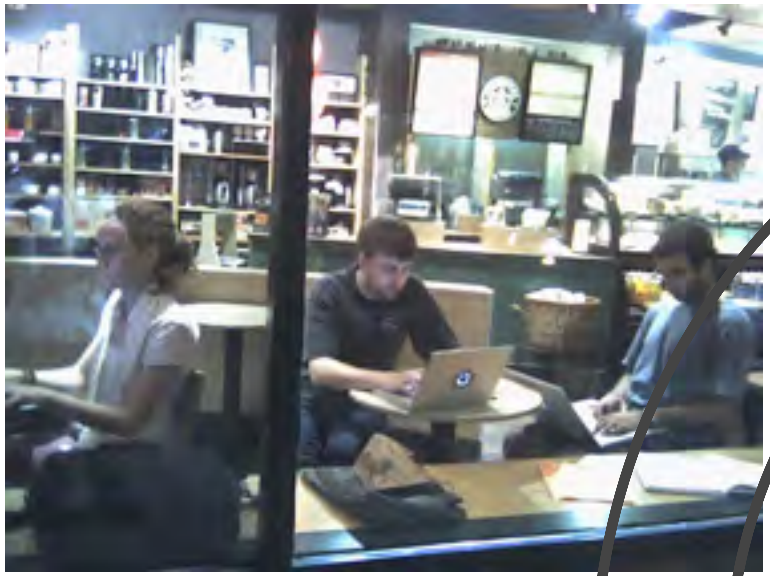


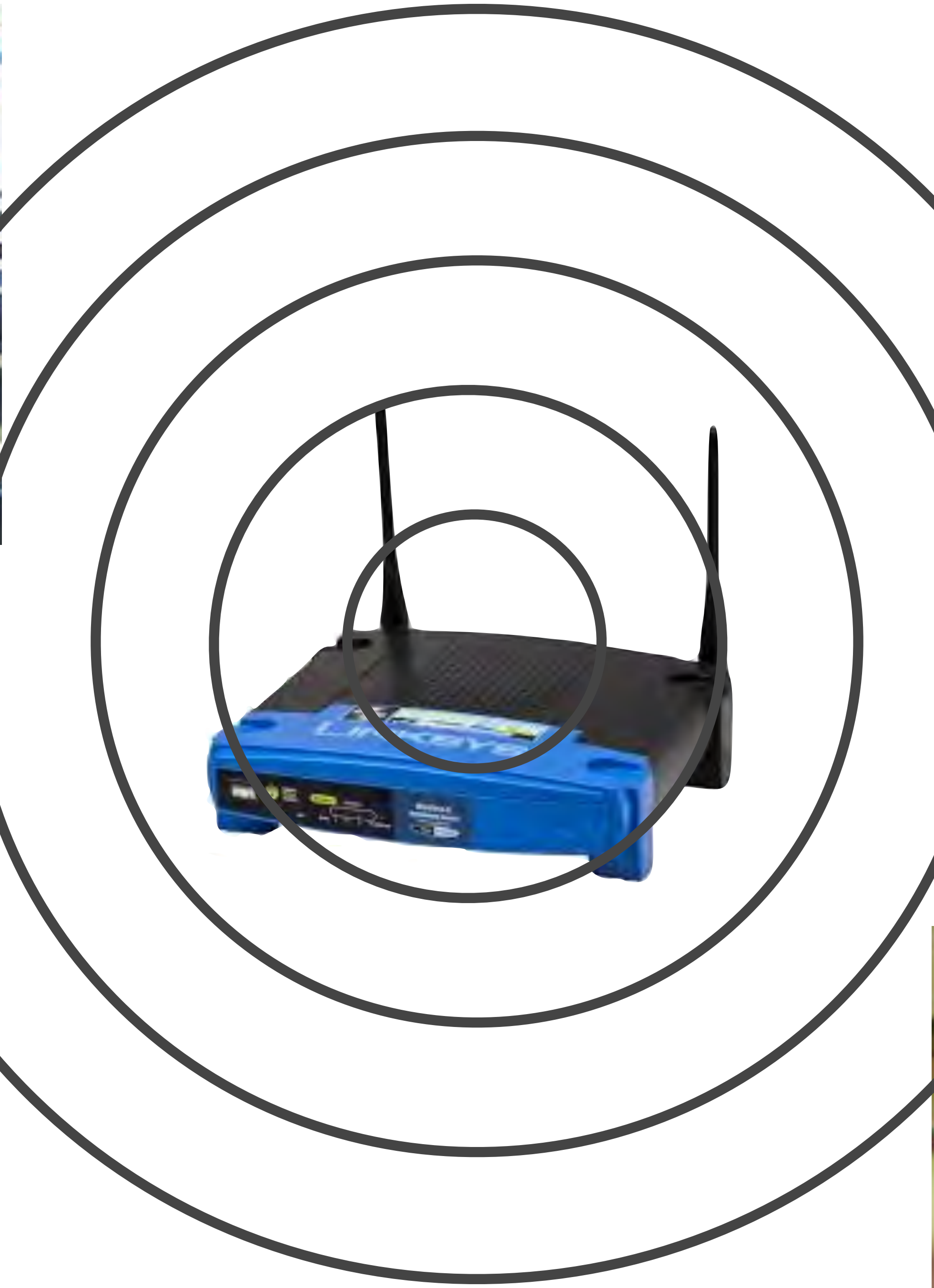
http://www.flickr.com/photos/superamit/45934256

Everybody in this room probably uses Wi-Fi.

(But hopefully not right now.)

Wi-Fi uses radio waves.
Radio waves move in all directions.





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

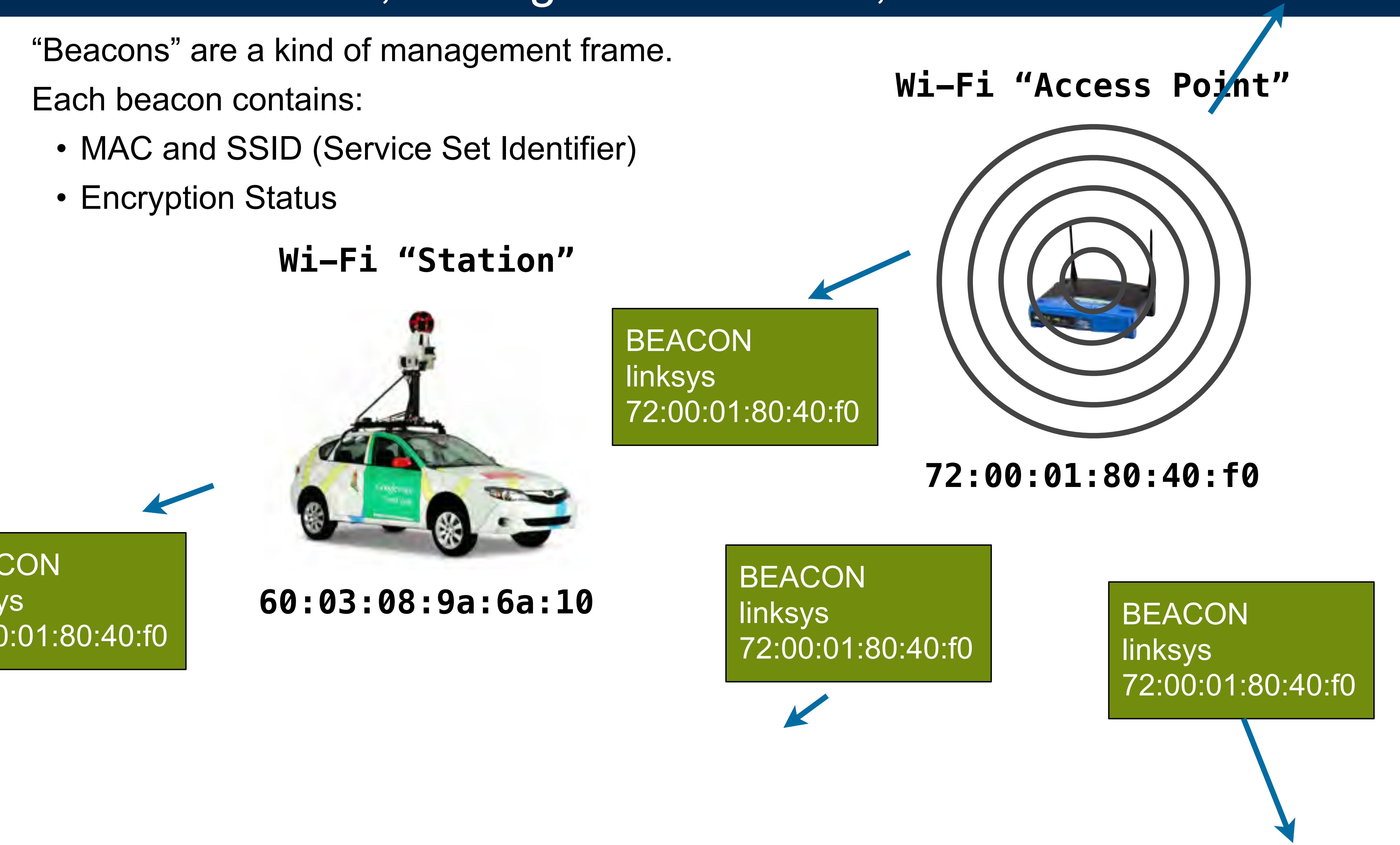
http://www.flickr.com/photos/orinrobertjohn/902282459

Wi-Fi Access Points send three kinds of packets: Control Frames, Management Frames, & Data Frames.

“Beacons” are a kind of management frame.

Each beacon contains:

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



Wi-Fi “Access Point”

72:00:01:80:40:f0

Wi-Fi “Station”

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

BEAC
linksys
72:00:

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

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

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

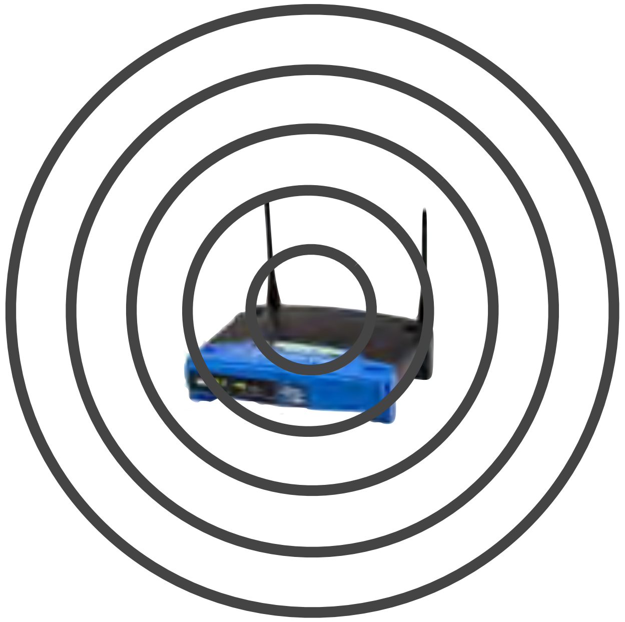
CON
ys
0:01:80:40:f0

Google's cars recorded Wi-Fi beacons & GPS coordinates.

Wi-Fi "Station"

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

Wi-Fi "Access Point"



`72:00:01:80:40:f0`

BEACON
I
7

BEACON
a
7

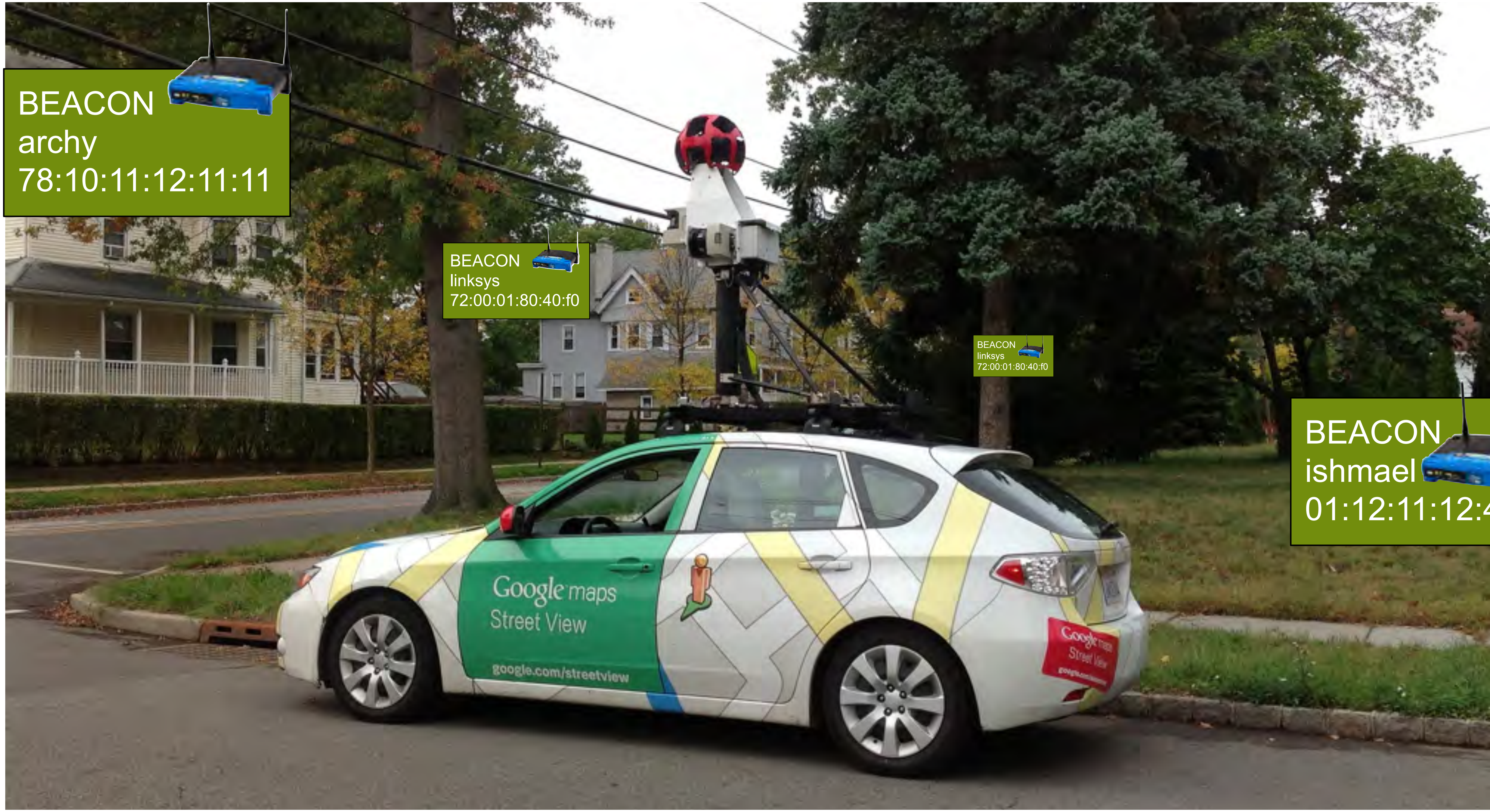
BEACON
ishmael
72:00:01:80:40:f0

0873, -74.0534

0.6083, -74.1533

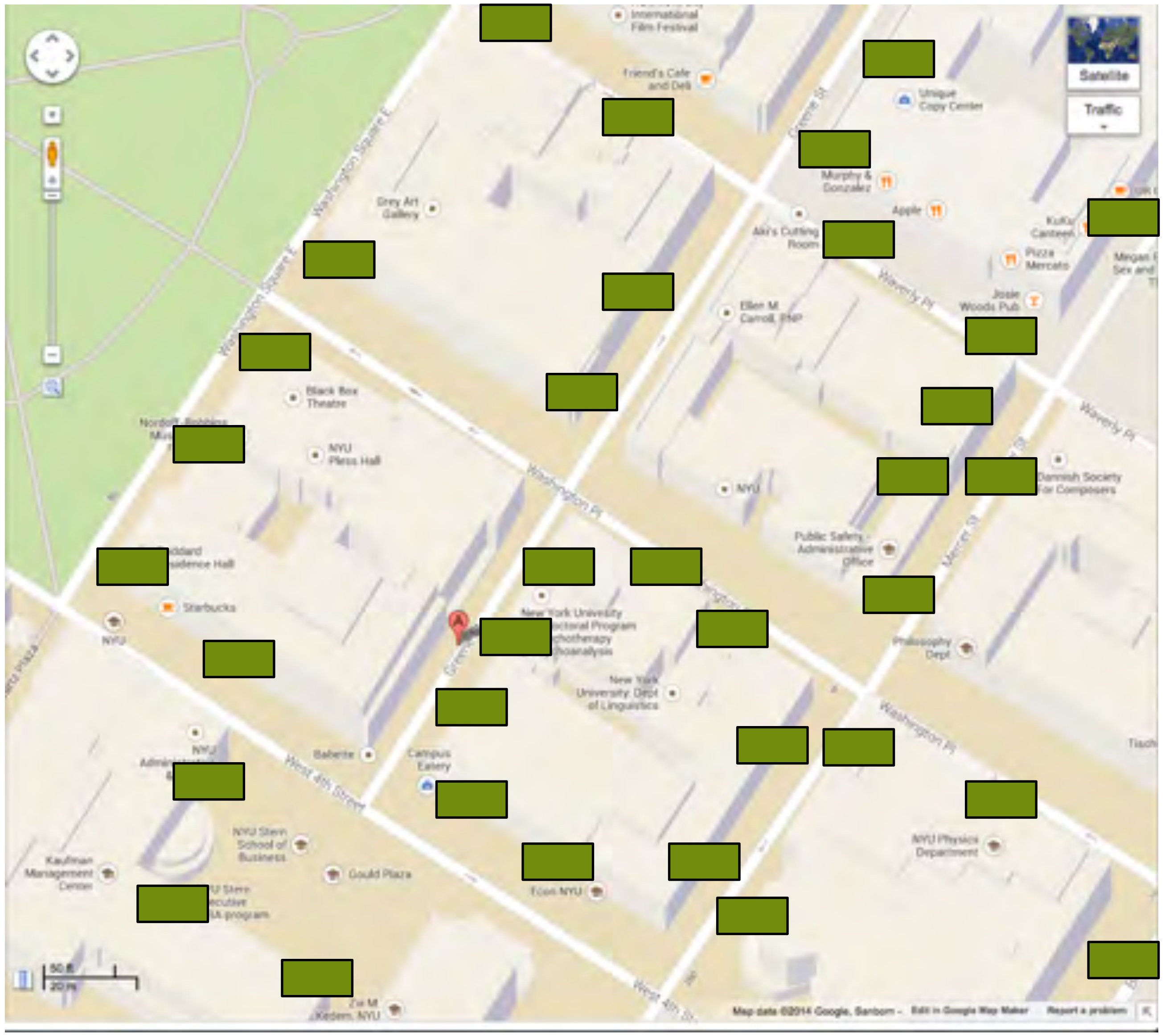
40.6123, -74.1542

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.

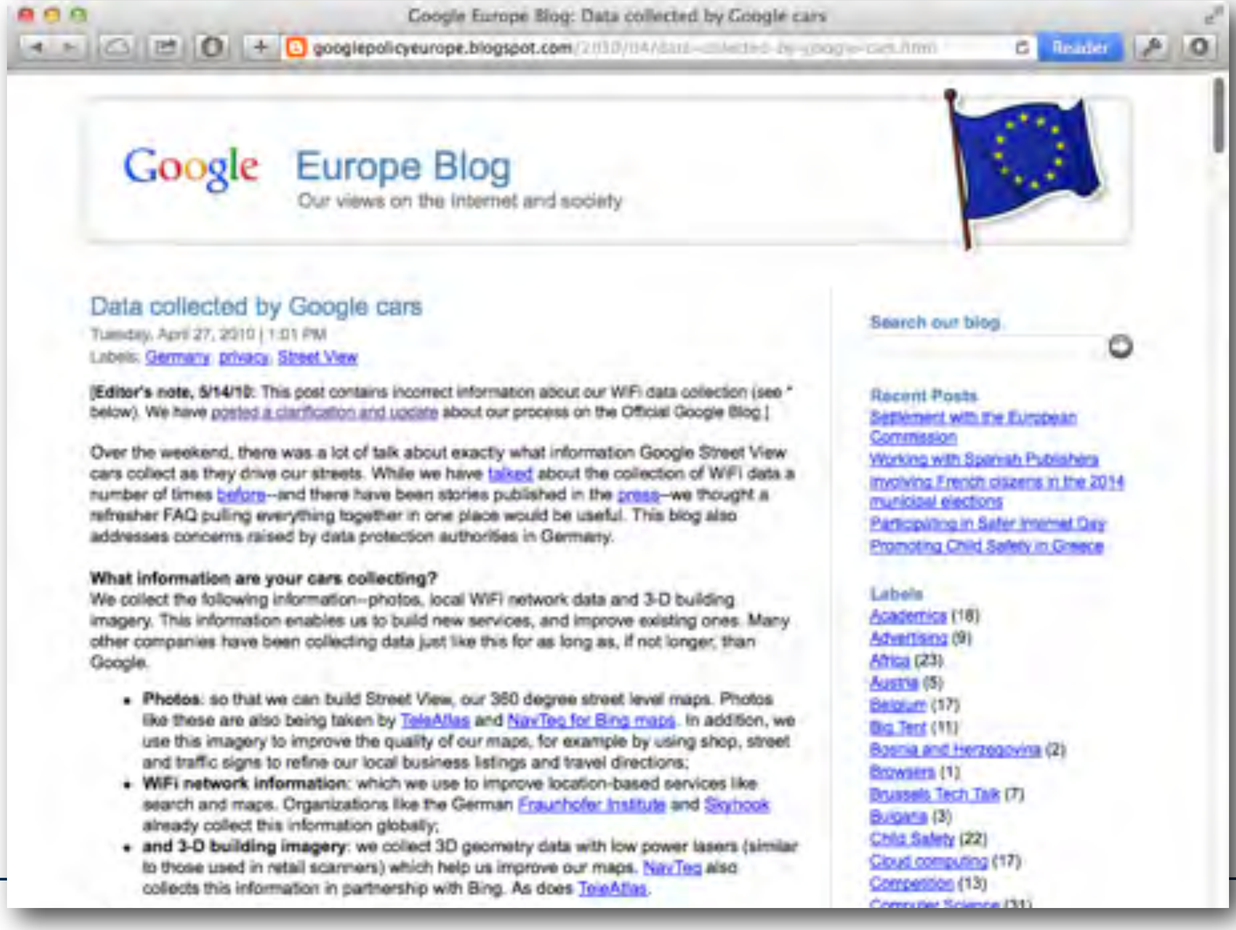
Google discovered that it was also capturing data frames.

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

- http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html

May 17, 2010 — Google announces that Irish Data Protection Authority asked Google to delete “payload data we collected in error in Ireland”

- http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html


Google Europe Blog: Data collected by Google cars
googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html
Reader

Google Europe Blog

Our views on the Internet and society

Data collected by Google cars

Tuesday, April 27, 2010 | 1:01 PM

Labels: Germany, privacy, Street View

[**Editor's note, 5/14/10**: This post contains incorrect information about our WiFi data collection (see * below). We have posted a clarification and update about our process on the Official Google Blog.]

Over the weekend, there was a lot of talk about exactly what information Google Street View cars collect as they drive our streets. While we have talked about the collection of WiFi data a number of times before--and there have been stories published in the press--we thought a refresher FAQ pulling everything together in one place would be useful. This blog also addresses concerns raised by data protection authorities in Germany.

What information are your cars collecting?

We collect the following information--photos, local WiFi network data and 3-D building imagery. This information enables us to build new services, and improve existing ones. Many other companies have been collecting data just like this for as long as, if not longer, than Google.

- **Photos**: so that we can build Street View, our 360 degree street level maps. Photos like these are also being taken by TeleAtlas and NavTeq for Bing maps. In addition, we use this imagery to improve the quality of our maps, for example by using shop, street and traffic signs to refine our local business listings and travel directions;
- **WiFi network information**: which we use to improve location-based services like search and maps. Organizations like the German Fraunhofer Institute and Skyhook already collect this information globally;
- **and 3-D building imagery**: we collect 3D geometry data with low power lasers (similar to those used in retail scanners) which help us improve our maps. NavTeq also collects this information in partnership with Bing. As does TeleAtlas.

Search our blog

Recent Posts

Settlement with the European Commission

Working with Spanish Publishers

Involving French citizens in the 2014 municipal elections

Participating in Safer Internet Day

Promoting Child Safety in Greece

Labels

Academics (18)
Advertising (9)
Africa (23)
Austria (5)
Belgium (17)
Big Tent (11)
Bosnia and Herzegovina (2)
Browsers (1)
Brussels Tech Talk (7)
Bulgaria (3)
Child Safety (22)
Cloud computing (17)
Competition (13)
Computer Science (31)

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:

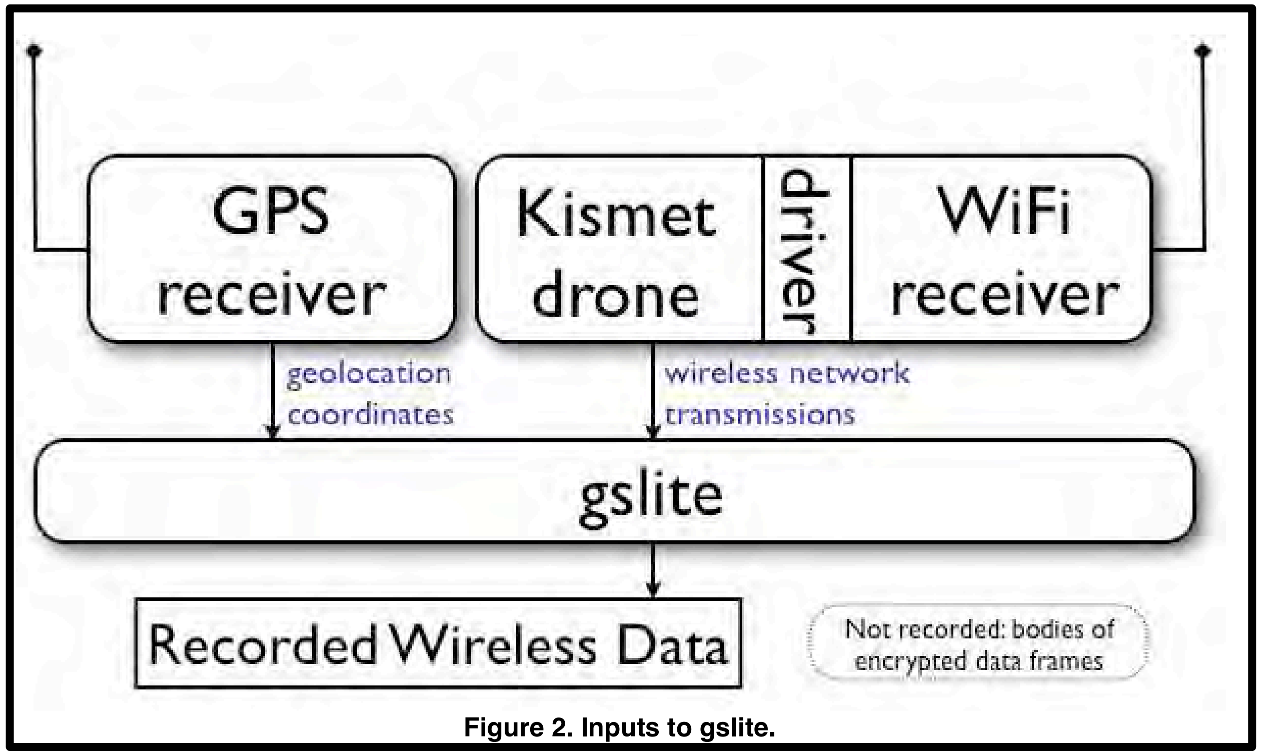
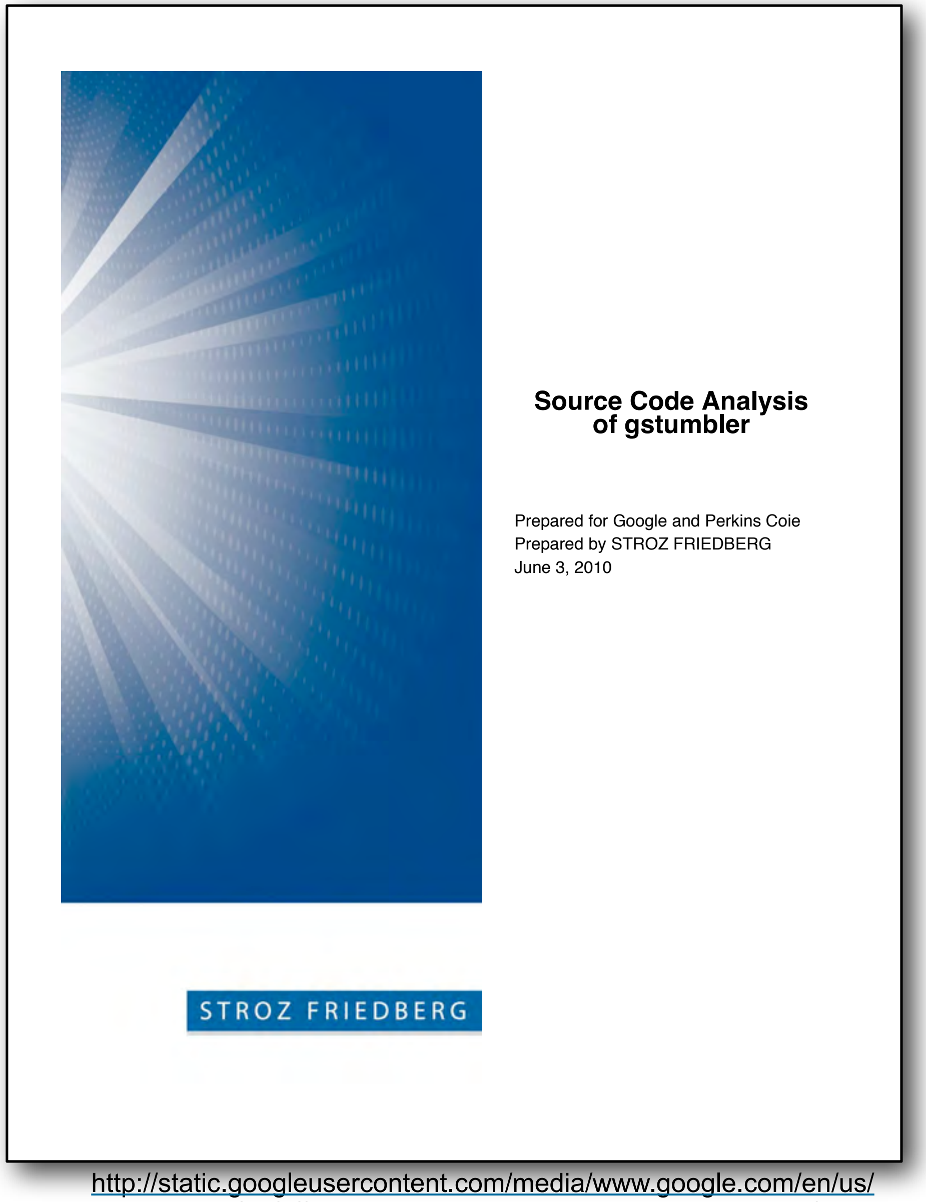


Figure 2. Inputs to gslite.



Source Code Analysis of gstumbler

Prepared for Google and Perkins Coie
Prepared by STROZ FRIEDBERG
June 3, 2010

STROZ FRIEDBERG

http://static.googleusercontent.com/media/www.google.com/en/us/googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf

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.’ ”

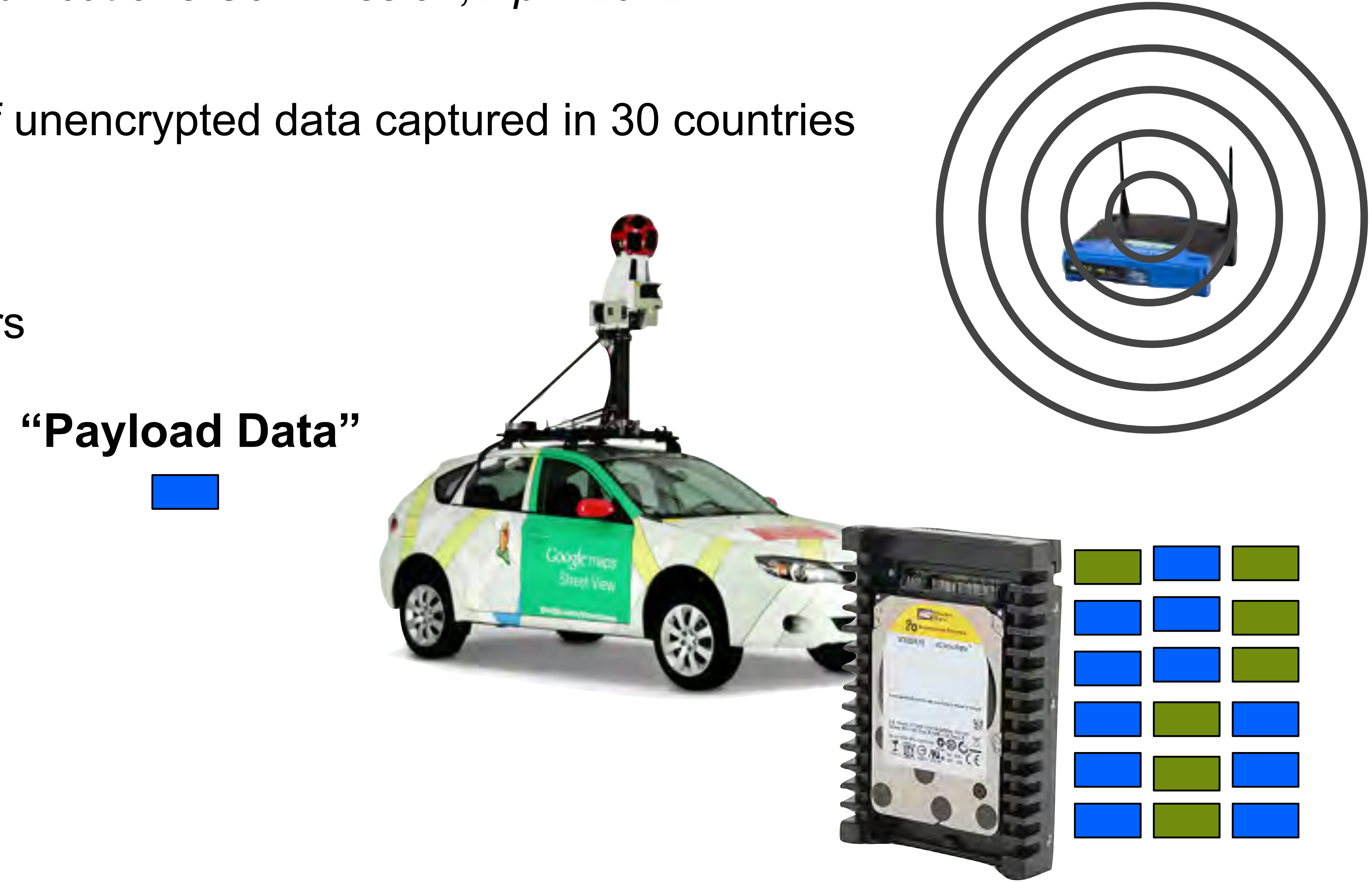
FCC’s conclusion: lots of data were collected.

“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.

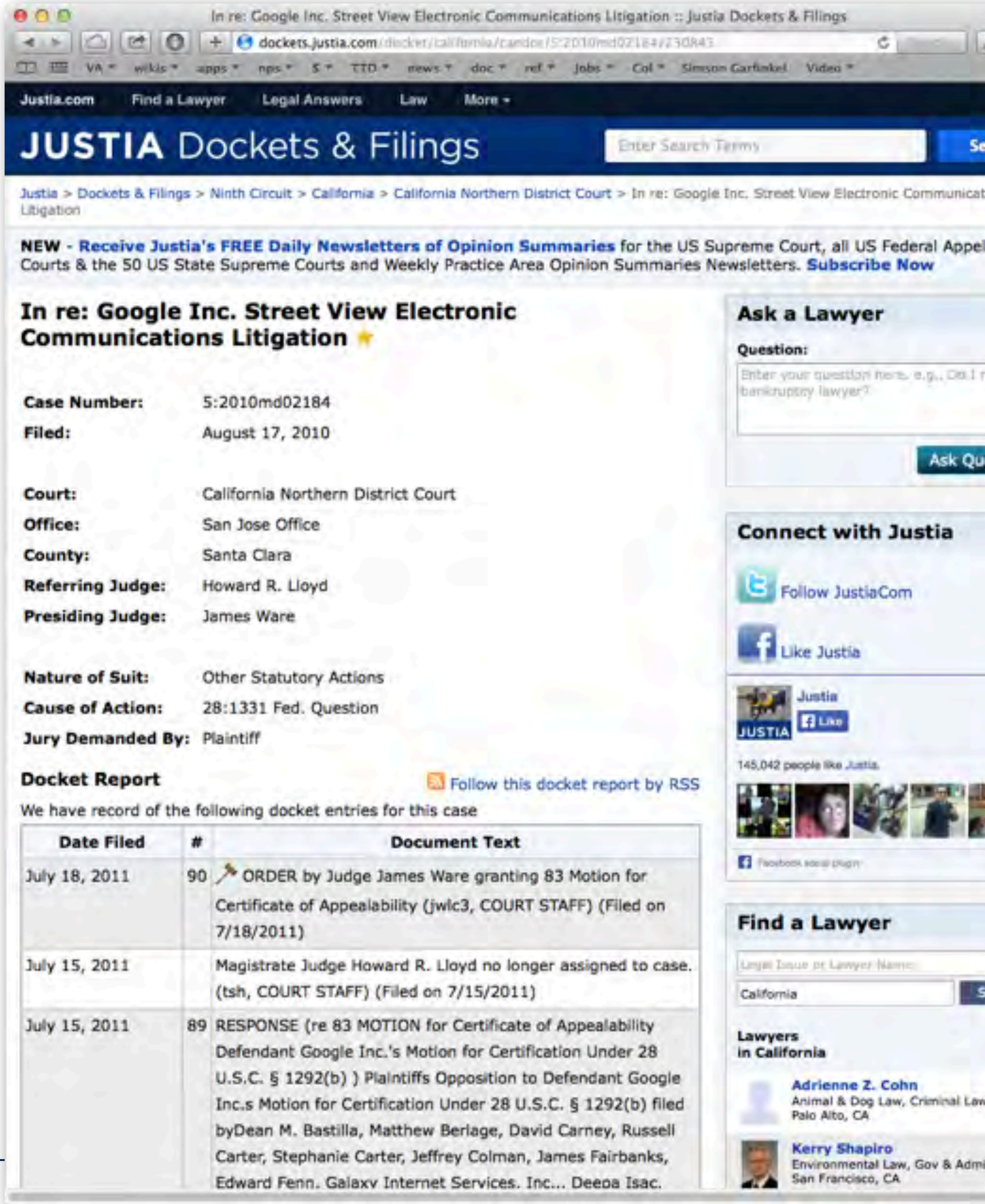
Several class-lawsuits were filed against Google. Consolidated in *Joffe v. Google (5:10-md-02184-JW)*

August 17, 2010

- Transferred to CA Northern District.

December 17, 2010

- Google files **Motion to Dismiss**


In re: Google Inc. Street View Electronic Communications Litigation :: Justia Dockets & Filings
dockets.justia.com
VA wikis apps nps $ TTD news doc ref Jobs Col Simson Garfinkel Video
Justia.com Find a Lawyer Legal Answers Law More
JUSTIA Dockets & Filings
Enter Search Terms
Justia > Dockets & Filings > Ninth Circuit > California > California Northern District Court > In re: Google Inc. Street View Electronic Communicat Litigation
Ask a Lawyer
Question:
Enter your question here, e.g., Do I r bankruptcy lawyer?
Ask Qu
Connect with Justia
Follow JustiaCom
Like Justia
Justia
Like
JUSTIA
145,042 people like Justia.
Facebook social plugin
Find a Lawyer
Legal Issue or Lawyer Name
California
Lawyers in California
Adrienne Z. Cohn
Animal & Dog Law, Criminal Law
Palo Alto, CA
Kerry Shapiro
Environmental Law, Gov & Admi
San Francisco, CA

NEW - **Receive Justia's FREE Daily Newsletters of Opinion Summaries** for the US Supreme Court, all US Federal Appel Courts & the 50 US State Supreme Courts and Weekly Practice Area Opinion Summaries Newsletters. **Subscribe Now**

In re: Google Inc. Street View Electronic Communications Litigation

Case Number:	5:2010md02184
Filed:	August 17, 2010
Court:	California Northern District Court
Office:	San Jose Office
County:	Santa Clara
Referring Judge:	Howard R. Lloyd
Presiding Judge:	James Ware
Nature of Suit:	Other Statutory Actions
Cause of Action:	28:1331 Fed. Question
Jury Demanded By:	Plaintiff

Docket Report

Follow this docket report by RSS

We have record of the following docket entries for this case

Date Filed	#	Document Text
July 18, 2011	90	ORDER by Judge James Ware granting 83 Motion for Certificate of Appealability (jwlc3, COURT STAFF) (Filed on 7/18/2011)
July 15, 2011		Magistrate Judge Howard R. Lloyd no longer assigned to case. (tsh, COURT STAFF) (Filed on 7/15/2011)
July 15, 2011	89	RESPONSE (re 83 MOTION for Certificate of Appealability Defendant Google Inc.'s Motion for Certification Under 28 U.S.C. § 1292(b)) Plaintiffs Opposition to Defendant Google Inc.s Motion for Certification Under 28 U.S.C. § 1292(b) filed byDean M. Bastilla, Matthew Berlage, David Carney, Russell Carter, Stephanie Carter, Jeffrey Colman, James Fairbanks, Edward Fenn, Galaxy Internet Services, Inc.., Deepa Isac,

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

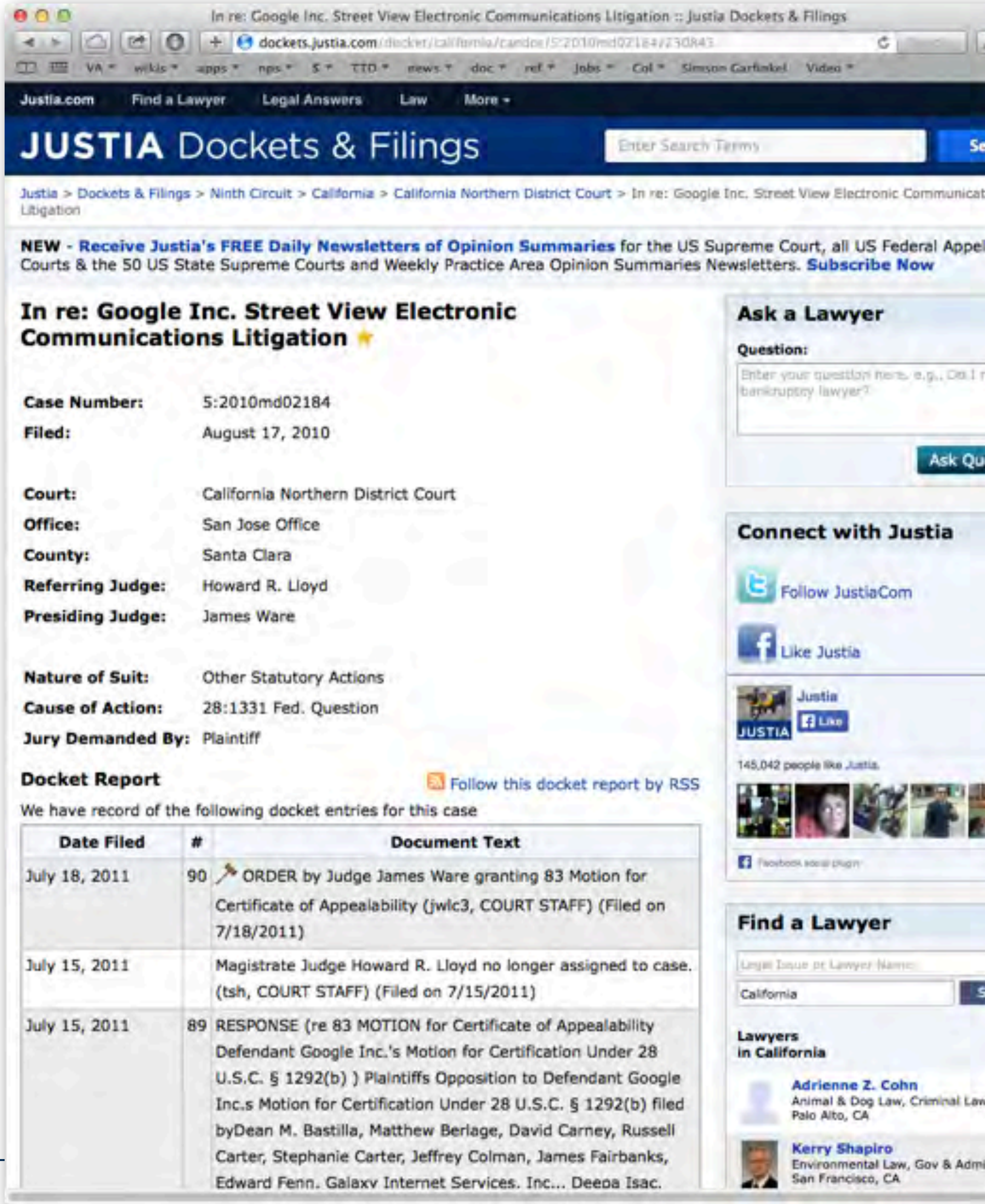
- ORDER granting in part and denying in part **Motion to Dismiss**

July 8, 2011

- Motion for a **Certificate of Appealability**

July 18, 2011

- Order granting **Certificate of Appealability**.


In re: Google Inc. Street View Electronic Communications Litigation :: Justia Dockets & Filings
dockets.justia.com/docket/california/candce/5:2010md02184/230843
VA
wikis
apps
nps
$
TTD
news
doc
ref
Jobs
Col
Simson Garfinkel
Video
Justia.com
Find a Lawyer
Legal Answers
Law
More
Enter Search Terms
Se

JUSTIA Dockets & Filings

Justia > Dockets & Filings > Ninth Circuit > California > California Northern District Court > In re: Google Inc. Street View Electronic Communicat Litigation

NEW - **Receive Justia's FREE Daily Newsletters of Opinion Summaries** for the US Supreme Court, all US Federal Appel Courts & the 50 US State Supreme Courts and Weekly Practice Area Opinion Summaries Newsletters. **Subscribe Now**

In re: Google Inc. Street View Electronic Communications Litigation ★

Case Number:	5:2010md02184
Filed:	August 17, 2010
Court:	California Northern District Court
Office:	San Jose Office
County:	Santa Clara
Referring Judge:	Howard R. Lloyd
Presiding Judge:	James Ware
Nature of Suit:	Other Statutory Actions
Cause of Action:	28:1331 Fed. Question
Jury Demanded By:	Plaintiff

Docket Report

Follow this docket report by RSS

We have record of the following docket entries for this case

Date Filed	#	Document Text
July 18, 2011	90	ORDER by Judge James Ware granting 83 Motion for Certificate of Appealability (jwlc3, COURT STAFF) (Filed on 7/18/2011)
July 15, 2011		Magistrate Judge Howard R. Lloyd no longer assigned to case. (tsh, COURT STAFF) (Filed on 7/15/2011)
July 15, 2011	89	RESPONSE (re 83 MOTION for Certificate of Appealability Defendant Google Inc.'s Motion for Certification Under 28 U.S.C. § 1292(b)) Plaintiffs Opposition to Defendant Google Inc.s Motion for Certification Under 28 U.S.C. § 1292(b) filed byDean M. Bastilla, Matthew Berlage, David Carney, Russell Carter, Stephanie Carter, Jeffrey Colman, James Fairbanks, Edward Fenn. Galaxv Internet Services. Inc... Deepa Isac.

Ask a Lawyer

Question:

Enter your question here, e.g., Do I n bankruptcy lawyer?

Ask Qu

Connect with Justia

Follow JustiaCom

Like Justia

Justia

Like

145,042 people like Justia.

Facebook social plugin

Find a Lawyer

Legal Issue or Lawyer Name

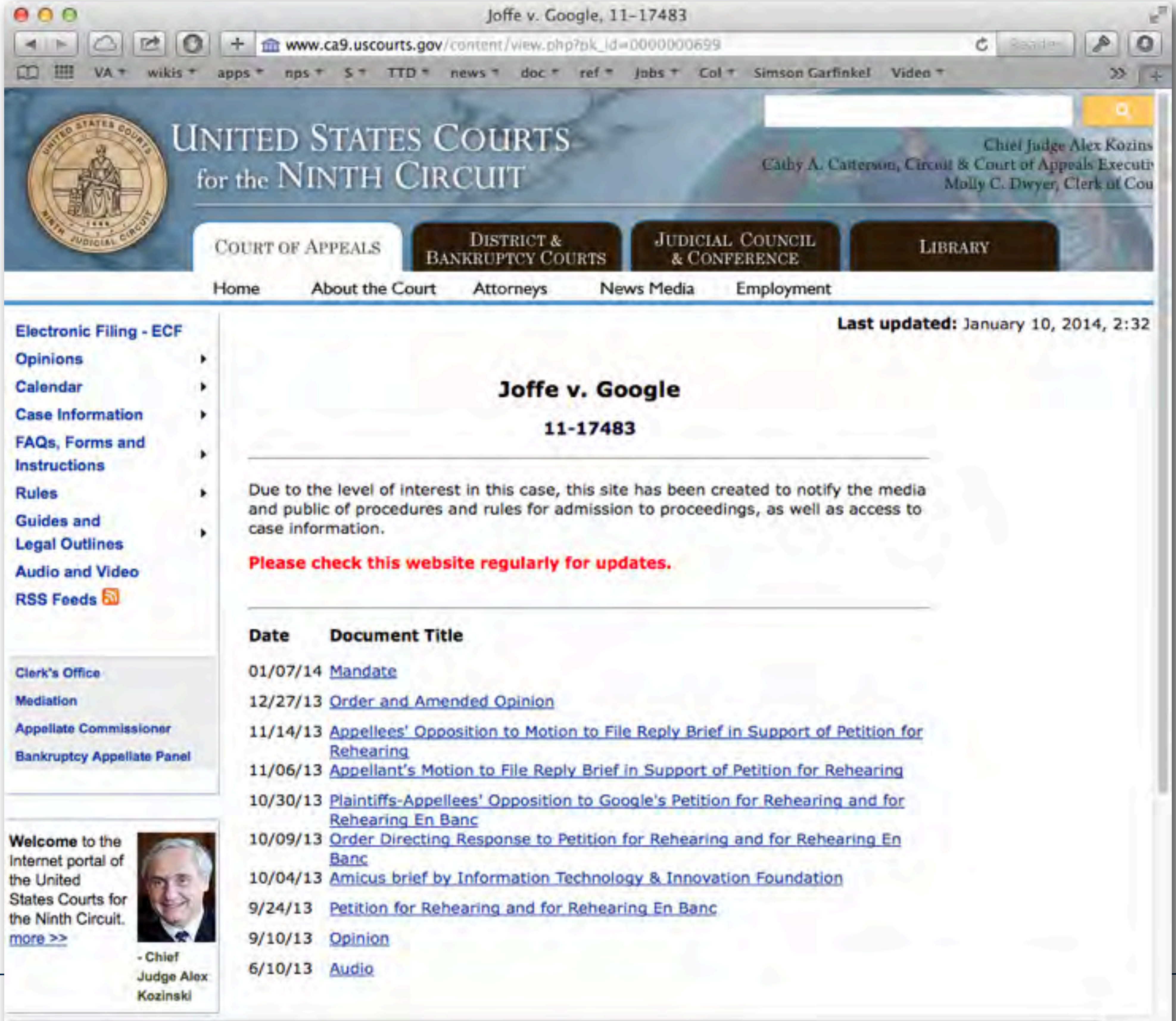
California

Lawyers in California

Adrienne Z. Cohn
Animal & Dog Law, Criminal Law
Palo Alto, CA

Kerry Shapiro
Environmental Law, Gov & Admi
San Francisco, CA

Google appealed the partial denial of its motion to dismiss to the US Courts for the Ninth Circuit.


Joffe v. Google, 11-17483
www.ca9.uscourts.gov/content/view.php?pk_id=0000000699
Reader
VA
wikis
apps
nps
$
TTD
news
doc
ref
Jobs
Col
Simson Garfinkel
Video
UNITED STATES COURTS for the NINTH CIRCUIT
Chief Judge Alex Kozinski
Cathy A. Catterson, Circuit & Court of Appeals Executi
Molly C. Dwyer, Clerk of Cou
COURT OF APPEALS
DISTRICT & BANKRUPTCY COURTS
JUDICIAL COUNCIL & CONFERENCE
LIBRARY
Home
About the Court
Attorneys
News Media
Employment
Electronic Filing - ECF
Opinions
Calendar
Case Information
FAQs, Forms and Instructions
Rules
Guides and Legal Outlines
Audio and Video
RSS Feeds
Clerk's Office
Mediation
Appellate Commissioner
Bankruptcy Appellate Panel

Welcome to the Internet portal of the United States Courts for the Ninth Circuit. more >>

- Chief Judge Alex Kozinski

Last updated: January 10, 2014, 2:32

Joffe v. Google

11-17483

Due to the level of interest in this case, this site has been created to notify the media and public of procedures and rules for admission to proceedings, as well as access to case information.

Please check this website regularly for updates.

Date	Document Title
01/07/14	Mandate
12/27/13	Order and Amended Opinion
11/14/13	Appellees' Opposition to Motion to File Reply Brief in Support of Petition for Rehearing
11/06/13	Appellant's Motion to File Reply Brief in Support of Petition for Rehearing
10/30/13	Plaintiffs-Appellees' Opposition to Google's Petition for Rehearing and for Rehearing En Banc
10/09/13	Order Directing Response to Petition for Rehearing and for Rehearing En Banc
10/04/13	Amicus brief by Information Technology & Innovation Foundation
9/24/13	Petition for Rehearing and for Rehearing En Banc
9/10/13	Opinion
6/10/13	Audio

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."~~

—*http://cdn.ca9.uscourts.gov/datastore/opinions/2013/12/27/11-17483%20web%20corrected.pdf*

http://en.wikipedia.org/wiki/Macintosh_Plus

The Wiretap Act

A bit more background on the law

The 1986 Electronic Communications Privacy Act was drafted in part to protect cell phone communications.

1983 — Motorola’s Dynatax 800x is receives FCC approval.

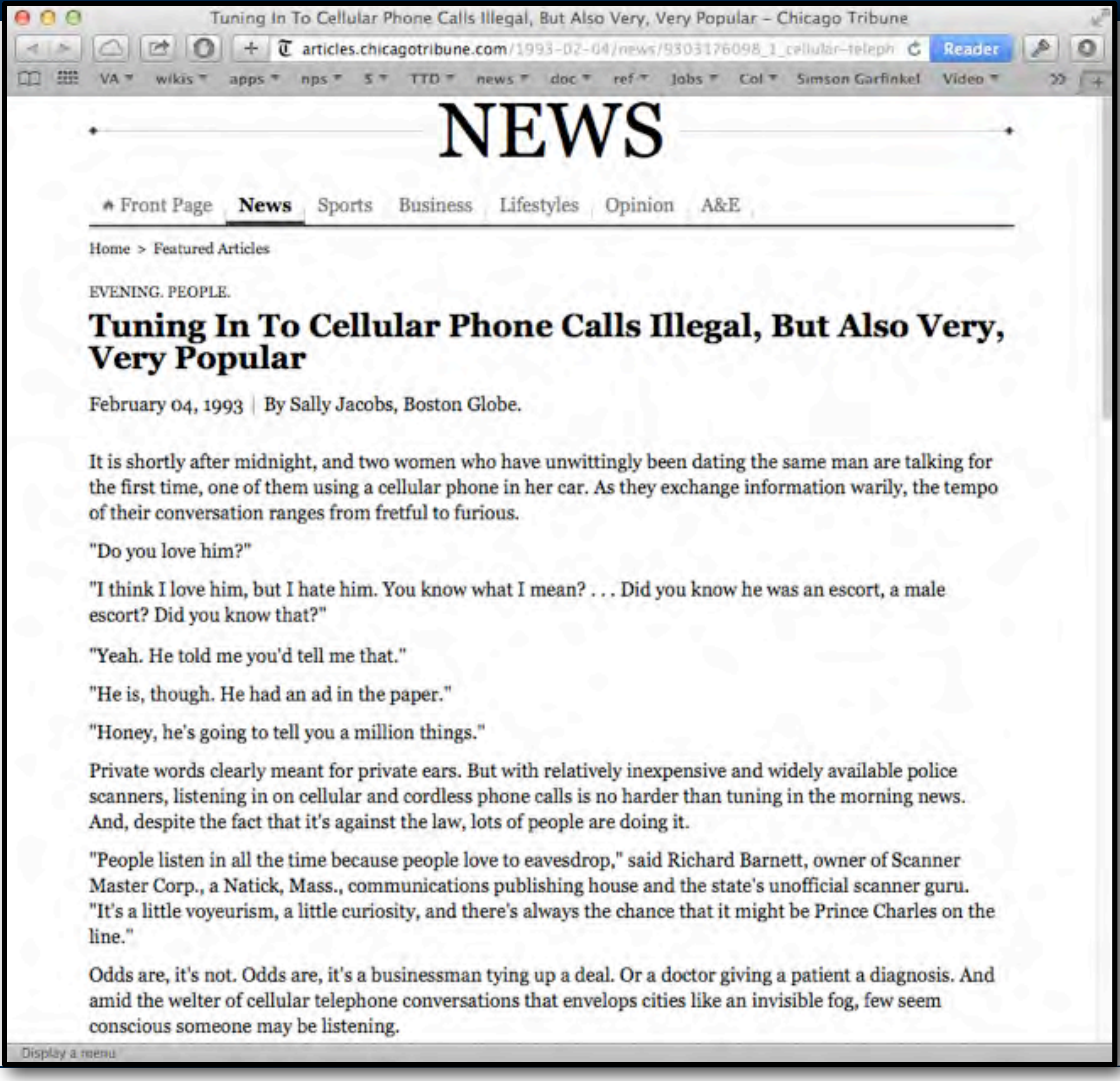
- AMPS — Advanced Mobile Phone System
- 850 MHz in US
- Analog
- No encryption
  - —*Monitoring by scanners*
  - —*Phone cloning (1990s)*

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)

http://en.wikipedia.org/wiki/File:DynaTAC8000X.jpg

Despite being illegal, many people listened …


Tuning In To Cellular Phone Calls Illegal, But Also Very, Very Popular – Chicago Tribune
articles.chicagotribune.com/1993-02-04/news/9303176098_1_cellular-teleph
Reader
VA
wikis
apps
nps
5
TTD
news
doc
ref
Jobs
Col
Simson Garfinkel
Video
Display a menu

NEWS

Front Page | News | Sports | Business | Lifestyles | Opinion | A&E

Home > Featured Articles

EVENING. PEOPLE.

Tuning In To Cellular Phone Calls Illegal, But Also Very, Very Popular

February 04, 1993 | By Sally Jacobs, Boston Globe.

It is shortly after midnight, and two women who have unwittingly been dating the same man are talking for the first time, one of them using a cellular phone in her car. As they exchange information warily, the tempo of their conversation ranges from fretful to furious.

"Do you love him?"

"I think I love him, but I hate him. You know what I mean? . . . Did you know he was an escort, a male escort? Did you know that?"

"Yeah. He told me you'd tell me that."

"He is, though. He had an ad in the paper."

"Honey, he's going to tell you a million things."

Private words clearly meant for private ears. But with relatively inexpensive and widely available police scanners, listening in on cellular and cordless phone calls is no harder than tuning in the morning news. And, despite the fact that it's against the law, lots of people are doing it.

"People listen in all the time because people love to eavesdrop," said Richard Barnett, owner of Scanner Master Corp., a Natick, Mass., communications publishing house and the state's unofficial scanner guru. "It's a little voyeurism, a little curiosity, and there's always the chance that it might be Prince Charles on the line."

Odds are, it's not. Odds are, it's a businessman tying up a deal. Or a doctor giving a patient a diagnosis. And amid the welter of cellular telephone conversations that envelops cities like an invisible fog, few seem conscious someone may be listening.

ECPA criminalized *cell phone* eavesdropping, *but not cordless phone eavesdropping.*

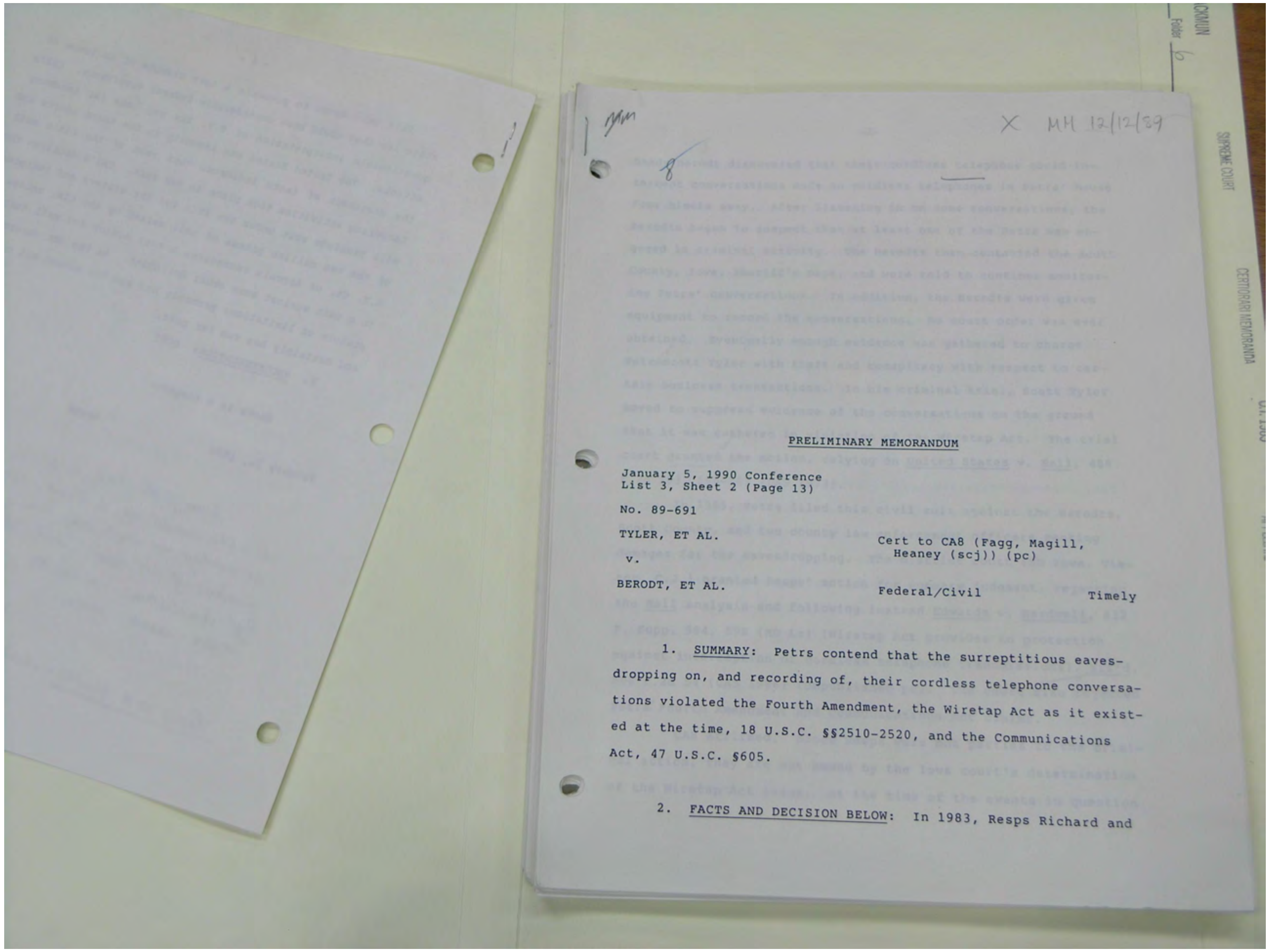
Illegal to sniff

Okay to sniff

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.



X MH 12/12/89

PRELIMINARY MEMORANDUM

January 5, 1990 Conference
List 3, Sheet 2 (Page 13)

No. 89-691

TYLER, ET AL.	Cert to CA8 (Fagg, Magill, Heaney (scj)) (pc)	
v.		
BERODT, ET AL.	Federal/Civil	Timely

1. SUMMARY: Petrs contend that the surreptitious eavesdropping on, and recording of, their cordless telephone conversations violated the Fourth Amendment, the Wiretap Act as it existed at the time, 18 U.S.C. §§2510-2520, and the Communications Act, 47 U.S.C. §605.

2. FACTS AND DECISION BELOW: In 1983, Resps Richard and

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.**

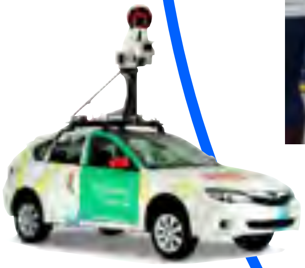
The 9th Circuit concluded that Wi-Fi is not “radio communication.”

—*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?



http://newyork.cbslocal.com/2013/10/31/police-investigating-violent-robbery-assault-at-nyu-building/

"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)

<u>You are totally correct 9th Circuit!</u>

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.*

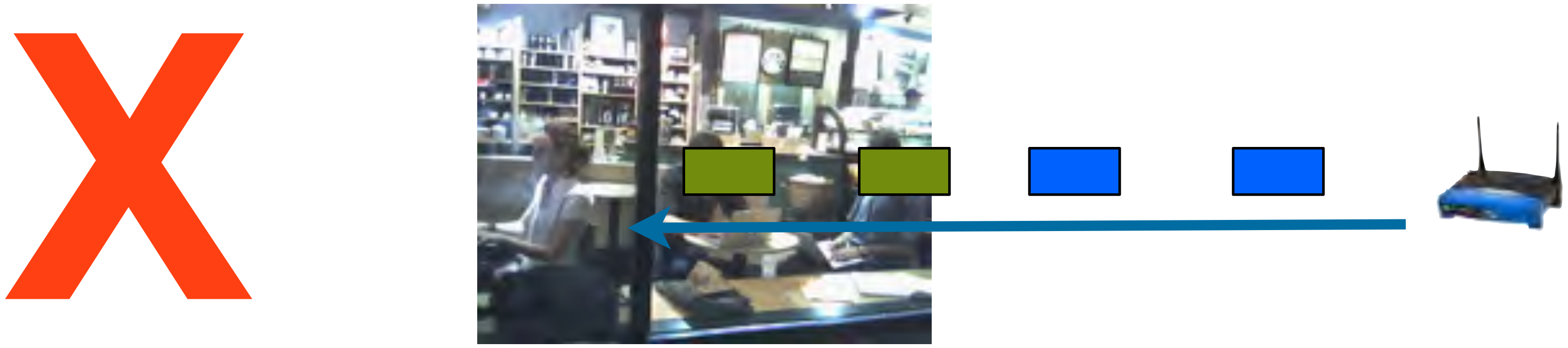
- —*“Because data packets sent over unencrypted Wi-Fi networks are readily accessible using the basic equipment described above, the Wiretap Act does not apply here.”*
- —*October 3, 2013.*
- —*http://sunsteinlaw.com/wp/wp-content/uploads/2013/11/Innovatio_Opinion.pdf*

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

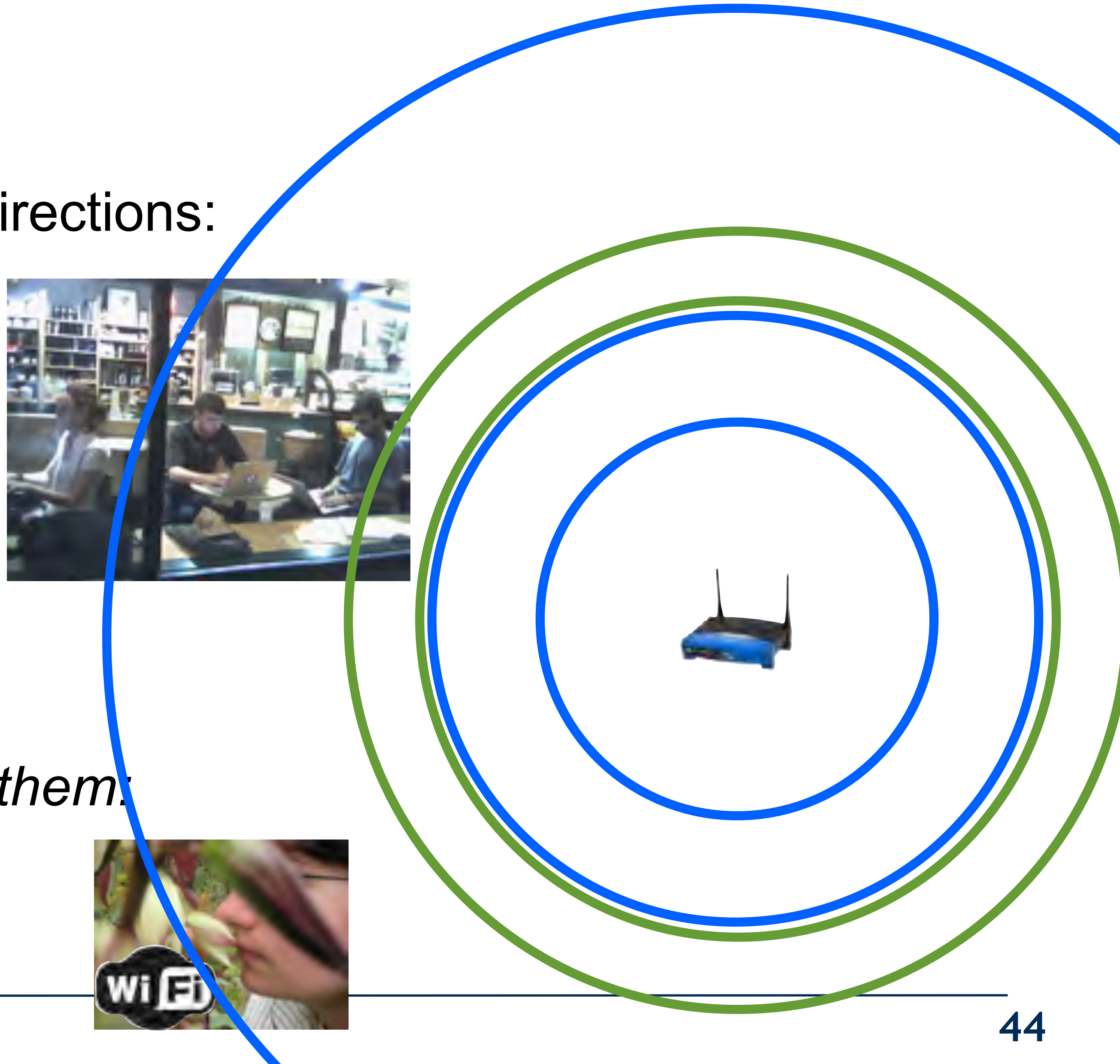
But — Wi-Fi sniffing will probably make its way to the Supreme Court.

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:



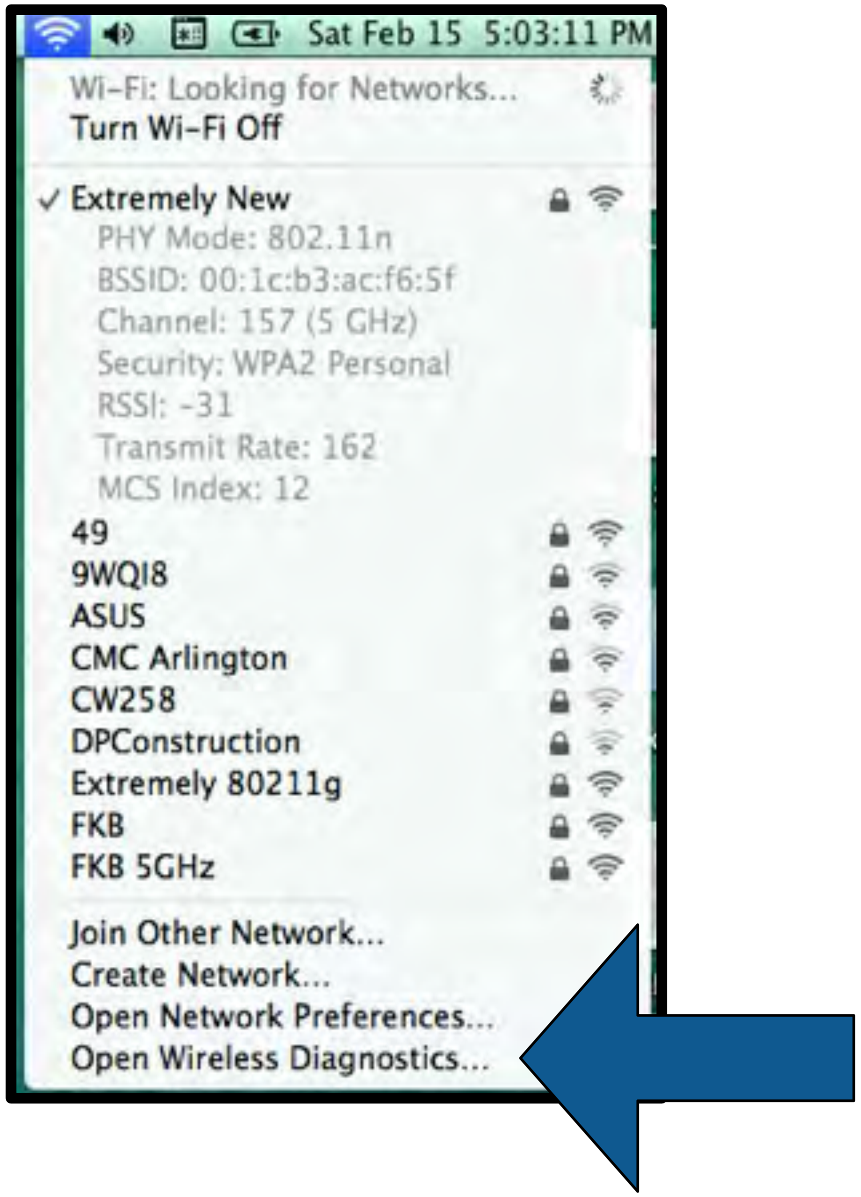
Packets actually travel in spherical shells in all directions:



—So it’s easy for another party to intercept them.

Wi-Fi capture software is widely available.

MacOS:



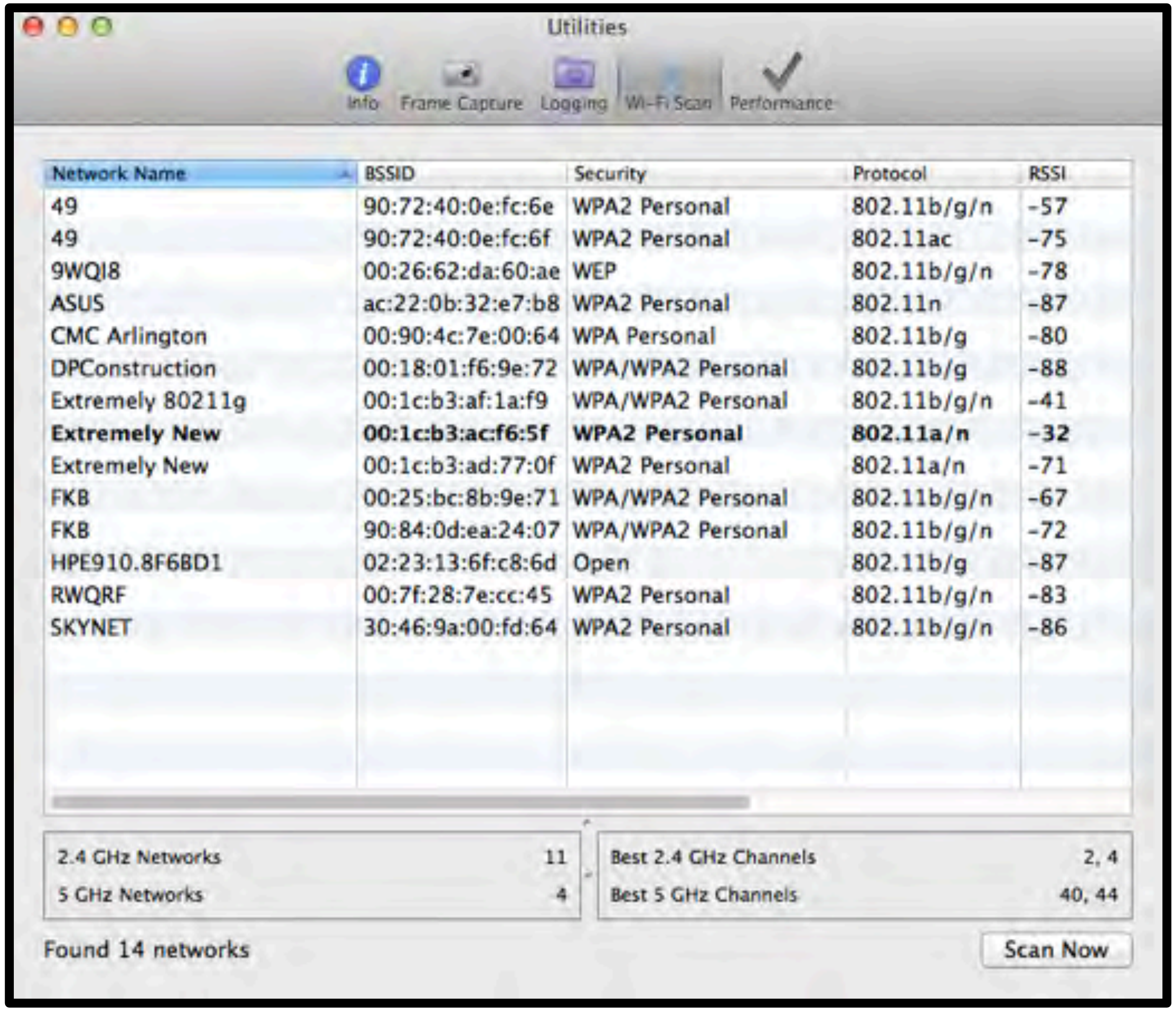
Sat Feb 15 5:03:11 PM

Wi-Fi: Looking for Networks...
Turn Wi-Fi Off

✓ Extremely New
PHY Mode: 802.11n
BSSID: 00:1c:b3:ac:f6:5f
Channel: 157 (5 GHz)
Security: WPA2 Personal
RSSI: -31
Transmit Rate: 162
MCS Index: 12

49
9WQI8
ASUS
CMC Arlington
CW258
DPConstruction
Extremely 80211g
FKB
FKB 5GHz

Join Other Network...
Create Network...
Open Network Preferences...
Open Wireless Diagnostics...

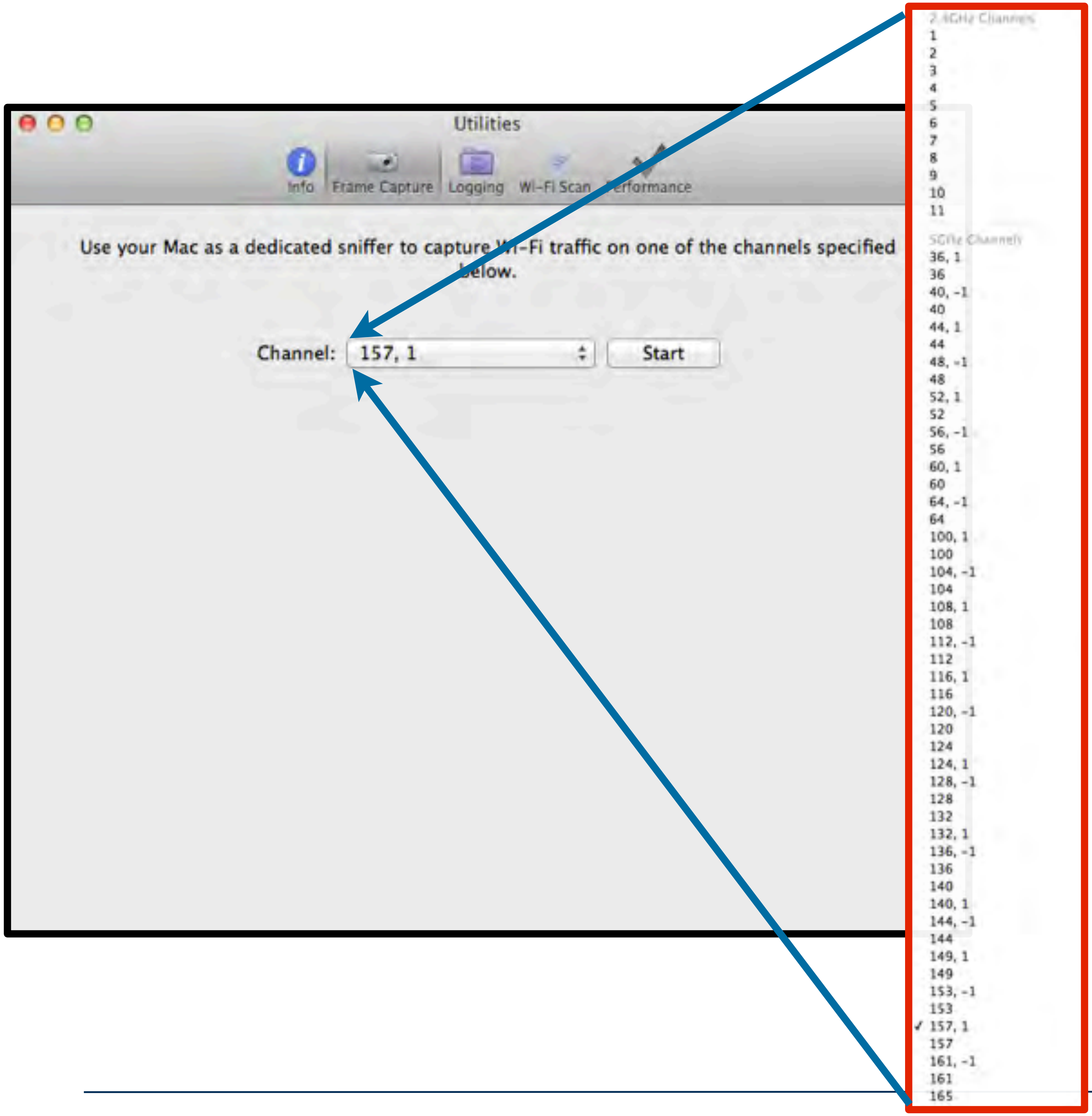


Network Name	BSSID	Security	Protocol	RSSI
49	90:72:40:0e:fc:6e	WPA2 Personal	802.11b/g/n	-57
49	90:72:40:0e:fc:6f	WPA2 Personal	802.11ac	-75
9WQI8	00:26:62:da:60:ae	WEP	802.11b/g/n	-78
ASUS	ac:22:0b:32:e7:b8	WPA2 Personal	802.11n	-87
CMC Arlington	00:90:4c:7e:00:64	WPA Personal	802.11b/g	-80
DPConstruction	00:18:01:f6:9e:72	WPA/WPA2 Personal	802.11b/g	-88
Extremely 80211g	00:1c:b3:af:1a:f9	WPA/WPA2 Personal	802.11b/g/n	-41
Extremely New	**00:1c:b3:ac:f6:5f**	**WPA2 Personal**	**802.11a/n**	**-32**
Extremely New	00:1c:b3:ad:77:0f	WPA2 Personal	802.11a/n	-71
FKB	00:25:bc:8b:9e:71	WPA/WPA2 Personal	802.11b/g/n	-67
FKB	90:84:0d:ea:24:07	WPA/WPA2 Personal	802.11b/g/n	-72
HPE910.8F6BD1	02:23:13:6f:c8:6d	Open	802.11b/g	-87
RWQRF	00:7f:28:7e:cc:45	WPA2 Personal	802.11b/g/n	-83
SKYNET	30:46:9a:00:fd:64	WPA2 Personal	802.11b/g/n	-86

2.4 GHz Networks	11
5 GHz Networks	4
Best 2.4 GHz Channels	2, 4
Best 5 GHz Channels	40, 44

Found 14 networks

Apple’s Sniffer can target any channel

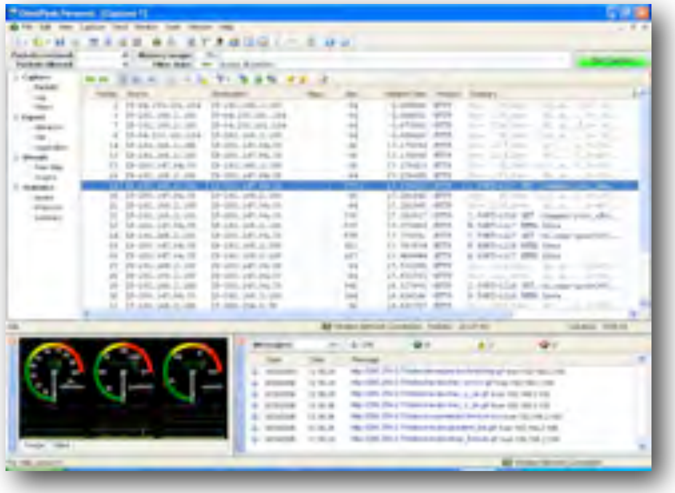


Use your Mac as a dedicated sniffer to capture Wi-Fi traffic on one of the channels specified below.

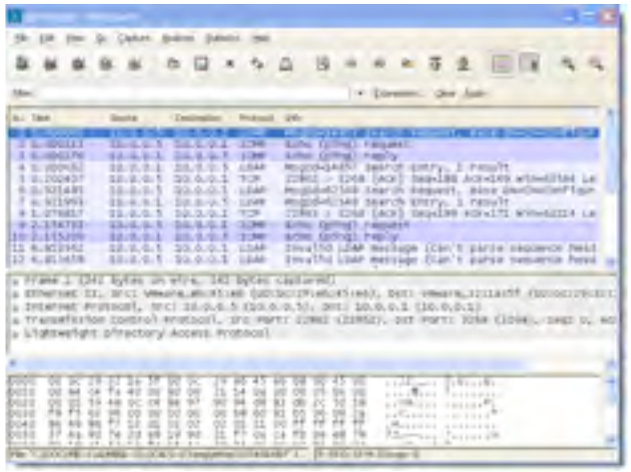
Channel: 157, 1

There are many programs for analyzing sniffed data

Wireshark and EtherPeek look at *packets*

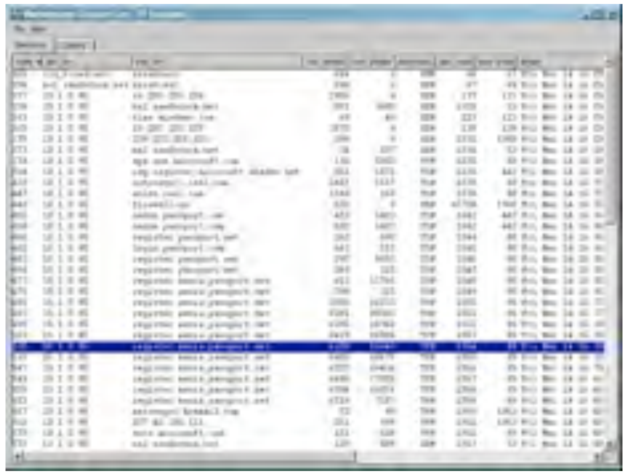


OmniPeek

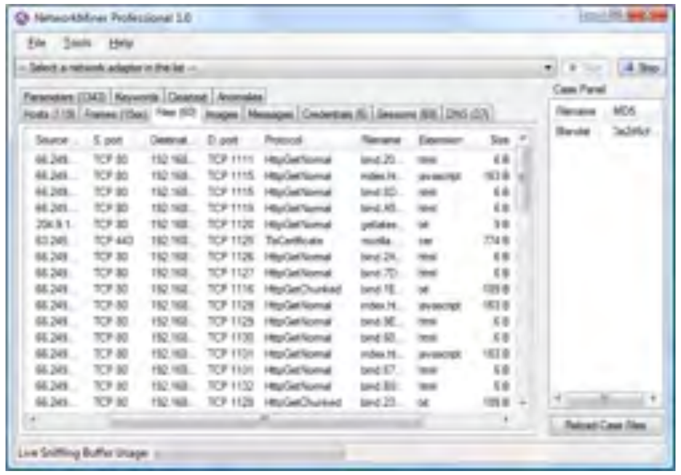


Wireshark

GUI-based tools can reconstruct entire web pages:



NetIntercept



NetworkMiner

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.

http://www.flickr.com/photos/jpellgen/3372418845

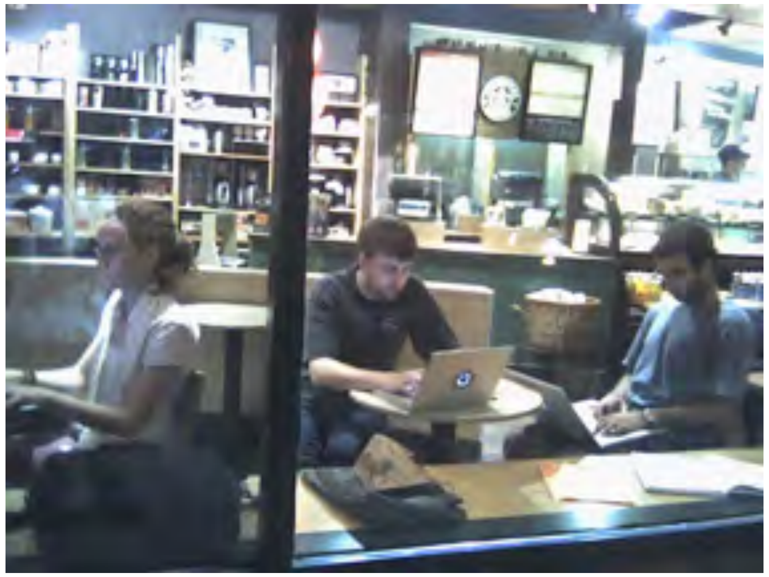
Implications for Education, Research and Technology

A bit more background

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:

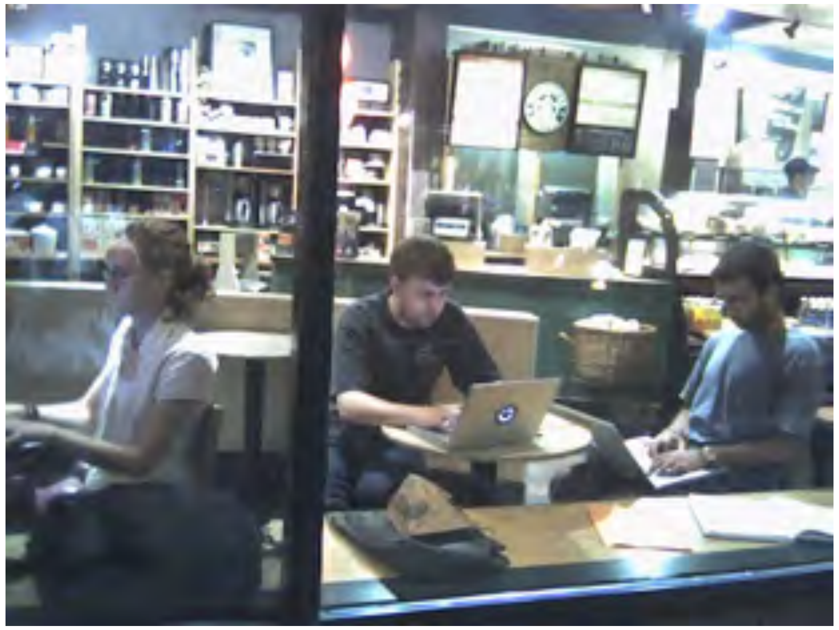
- Be careful about Wi-Fi surveys
- Don’t sniff at Starbucks

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*

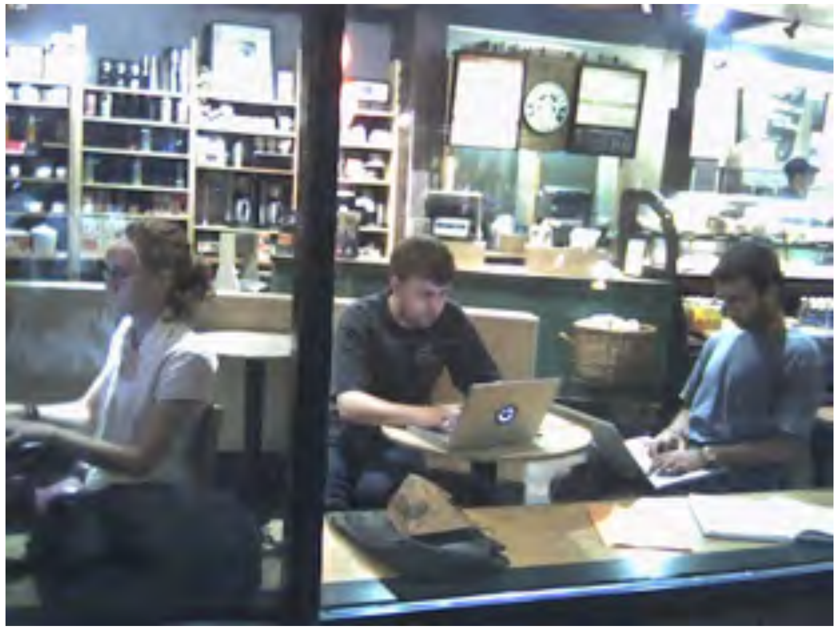
What is the right public policy?

Should it be legal to intercept their packets:



What is the right public policy?

Should it be legal to intercept their packets:



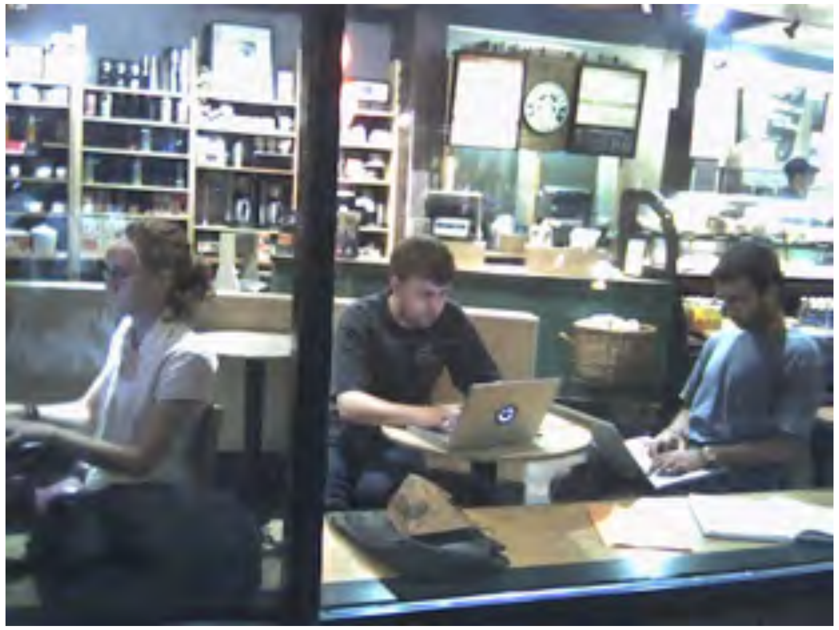
If it was 1988 and these people had wireless phones in the coffee shop...

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

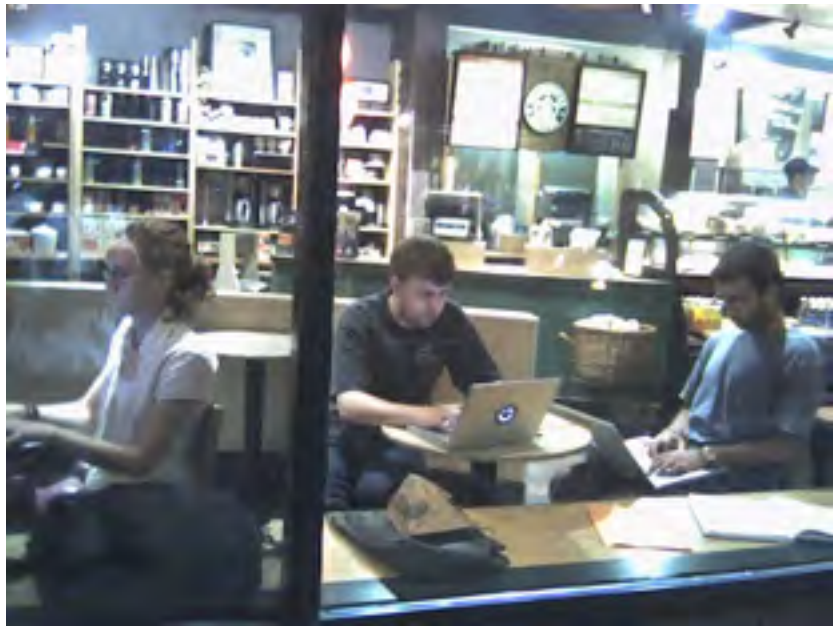
unlicensed

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

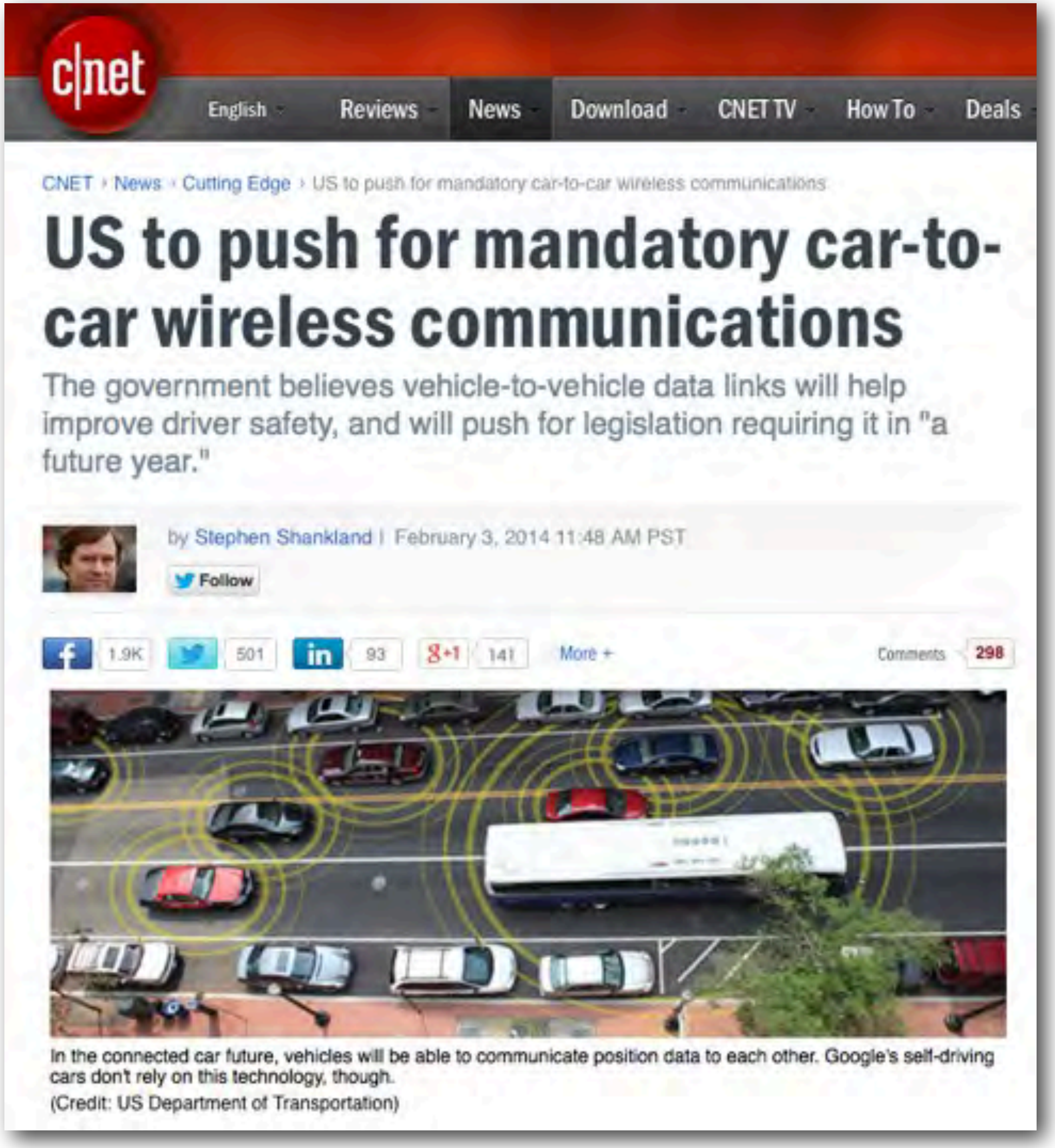
Illegal to sniff

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...



CNET › News › Cutting Edge › US to push for mandatory car-to-car wireless communications

US to push for mandatory car-to-car wireless communications

The government believes vehicle-to-vehicle data links will help improve driver safety, and will push for legislation requiring it in "a future year."

by Stephen Shankland | February 3, 2014 11:48 AM PST

In the connected car future, vehicles will be able to communicate position data to each other. Google's self-driving cars don't rely on this technology, though.
(Credit: US Department of Transportation)

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.

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

References

"Source Code Analysis of gstumbler", Stroz Friedberg, June 3, 2011

—*http://static.googleusercontent.com/media/www.google.com/en/us/googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf*

"Notice of Apparent Liability for Forfeiture," FCC DA 12-592, April 13, 2012

—*http://transition.fcc.gov/DA-12-592A1.pdf*

—*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,

—*http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000699*

WiFi data collection: An update, Google, May 2010

—*http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html*

Data Engineer in Google Case Is Identified, New York Times, April 30, 2012

—*http://www.nytimes.com/2012/05/01/technology/engineer-in-googles-street-view-is-identified.html*

Preliminary Memorandum, January 5, 1990 Conference, List 3, Sheet 2 (Page 13), No. 89-691, Tyler et al v. Berodt, Et al.

—*http://epstein.usc.edu/research/blackmunMemos/1989/DM-1989-pdf/89-691.pdf*