Scalable enforcement

Henning Schulzrinne
Columbia University

September 2018

New Jersey Man

3. On August 3, 2012, the Enforcement Bureau (Bureau) received a complaint from the Federal Aviation Administration (FAA) reporting that the Port Authority of New York and New Jersey (Port Authority) had been experiencing interference during pre-deployment testing of a ground-based augmentation system (GBAS) at Newark Liberty International Airport (Newark Airport).[7] The GBAS provides enhanced navigation signals to aircraft in the vicinity of an airport for precision approach, departure procedures, and terminal area operations.

4. An agent from the Bureau's New York Office investigated the matter at Newark Airport on August 4, 2012. While driving toward the Guard Post India Gate at the Newark Airport, the agent determined, using direction finding techniques, that a red Ford F-150 pickup truck with New Jersey license plates (Red Ford) was emanating radio signals within the restricted 1559 to 1610 MHz band allocated to the Radionavigation-Satellite service and used by the GPS satellite navigation system.[8] The signals emanating from the vehicle were blocking the reception of GPS signals by the GPS receivers used in the GBAS. Port Authority police and security personnel, working closely with the FCC agent, stopped the Red Ford at the gate. Using handheld direction finding equipment, the FCC agent confirmed that strong wide-band emissions in the restricted 1559 to 1610 MHz band were emanating from the Red Ford. The FCC agent interviewed the driver, who identified himself as Gary Bojczak and admitted that he owned and operated the radio transmitting device that was jamming GPS transmissions. Mr. Bojczak claimed that he installed and operated the jamming device in his company-supplied vehicle to block the GPS-based vehicle tracking system that his employer installed in the vehicle. Mr. Bojczak voluntarily surrendered the jammer to the FCC agent. After the jammer was removed from the Red Ford and turned off, the agent confirmed that the unauthorized signals had ceased.

LED lighting

Last year we reported on two cases, this one and this one, about FCC actions against users of commercial lighting that caused interference to cell 4G data service. In both cases, so far as we can tell, the fixtures were conventional fluorescents that produced radio noise unintentionally.

The FCC has now presented us with a variation on the theme. The fixtures here – "fluorescent lighting electronic ballasts" – are located in a large office building on South Figueroa in downtown Los Angeles. They're a specific kind that generate radio-frequency energy on purpose. Ideally the radio waves would stay trapped inside the device, but in practice some always leak out. Unlike most of the fixtures in our kitchens at home, this type is subject to specific FCC technical rules that limit the strength of escaping radio-frequency emissions. At 4G frequencies (and most other frequencies as well), the permitted levels are harmlessly low.

This time, though, the levels were high enough to cause interference to a nearby Verizon Wireless 700 MHz LTE cell site.

Verizon traced the problem to particular lights in the building and notified the building management. When the interference persisted, Verizon called in the FCC. The lighting manufacturer, GE, had previously issued a bulletin noting that some of its units produced excessive radio-frequency emissions. The FCC confirmed which units in the building were causing the trouble, found they were among those covered by the bulletin, and ordered the management to take corrective action. In practice, this typically means replacing the lights.

https://www.commlawblog.com/2014/02/articles/enforcement-activities-fines-forfeitures-etc/bulbs-behind-bars-iii-more-lighting-fixtures-mess-up-mobile-data-service/

U-NII

U-NII and TDWR Interference Enforcement

The Enforcement Bureau took the actions listed below against companies operating devices that caused interference to primary services operating within the Unlicensed National Information Infrastructure (U-NII) spectrum. Primary services operating within this spectrum include the Terminal Doppler Weather Radar (TDWR) systems operated by the Federal Aviation Administration (FAA), US Armed Forces and TV broadcast stations. TDWR systems serve the critical function of providing quantitative measurements for gust fronts, wind shear, microbursts, and other weather related hazards.

Investigations conducted by the FCC, the FAA, the U.S. Air Force and the National Telecommunications and Information Administration (NTIA) in several areas of the United States and Puerto Rico revealed that much of the interference stems from wireless devices sharing the same band as TDWR systems. These wireless transmitters are authorized on a secondary non-interfering basis under the FCC's Rules for U-NII. (See 47 C.F.R. Part 15 subpart E.) The FCC continues to investigate reports of interference to TDWR systems and other primary 5GHz band users, and will continue to take appropriate enforcement action when necessary.

The Enforcement Bureau and the Office of Engineering and Technology issued a memorandum to manufacturers and operators of U-NII devices concerning the elimination of interference to TDWR systems.

Enforcement Advisory - Wireless Internet Service Provider Guidance

Enforcement Actions

11-14-2017	RADWIN Ltd., RADWIN, Inc.	ORDER & CONSENT DECREE
09-16-2016	Airosurf Communications, Inc.,Edmond, Oklahoma	NOUO
07-29-2016	Towerstream Corporation, Middletown, Rhode Island	ORDER & CONSENT DECREE

Interference - means, motive & opportunity

unintentional
non-malicious

LED lighting

intentional
non-malicious
“nobody is harmed”

local GPS jamming

UNI DFS disabling
WISP power amplifiers

intentional
malicious
active evasion

no FCC equipment
authorization

GPS jamming

Stingray (foreign intelligence)

Scalable enforcement

Flow, a new air-quality sensor, and its companion app are displayed during a press event for CES 2017 on January 3, 2017 in Las Vegas. // David Becker/Getty Images

Cheap Sensors Are Democratizing Air-Quality Data

JASON PLAUTZ JUL 9, 2018

➔ network of spectrum sensors – but are they legal?

Automatic station identification ➔ may work for Wi-Fi and other intentional transmitters, but not noisy LEDs and GPS jammers

FCC field offices: 3 regions (Columbia, MD; Atlanta, GA; Los Angeles, CA) + Boston, MA; Chicago, IL; Columbia, MD; Dallas, TX; Denver, CO; Honolulu, HI; Miami, FL; New Orleans, LA; New York, NY; Portland, OR; and San Francisco, CA)
54 staff (GAO, 2017)

Intercept: 18 U.S. Code § 2511

- (1) Except as otherwise specifically provided in this chapter any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
  - (ii) such device transmits communications by radio, or interferes with the transmission of such communication; …
- **(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;
  - **(iv)** to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
  - **(v)** for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

18 U.S. Code § 2510 - Definitions

- **(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;

47 U.S. Code § 705

- No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto.

Google StreetView (2010-2012)

1. Between May 2007 and May 2010, as part of its Street View project, Google Inc. (Google or Company) collected data from Wi-Fi networks throughout the United States and around the world.[1] The purpose of Google's Wi-Fi data collection initiative was to capture information about Wi-Fi networks that the Company could use to help establish users' locations and provide location-based services. But Google also collected "payload" data—the content of Internet communications—that was not needed for its location database project. This payload data included e-mail and text messages, passwords, Internet usage history, and other highly sensitive personal information.

4. For many months, Google deliberately impeded and delayed the Bureau's investigation by failing to respond to requests for material information and to provide certifications and verifications of its responses. In this Notice of Apparent Liability for Forfeiture (NAL), we find that Google apparently willfully and repeatedly violated Commission orders to produce certain information and documents that the Commission required for its investigation. Based on our review of the facts and circumstances before us, we find that Google, which holds Commission licenses,[10] is apparently liable for a forfeiture penalty of $25,000 for its noncompliance with Bureau information and document requests.

5. At the same time, based on a careful review of the existing record and applicable law, the Bureau will not take enforcement action under Section 705(a) against the Company for its collection of payload data. There is not clear precedent for applying Section 705(a) of the Communications Act to the Wi-Fi communications at issue here. Moreover, because Engineer Doe permissibly asserted his constitutional right not to testify, significant factual questions bearing on the application of Section 705(a) to the Street View project cannot be answered on the record of this investigation.

Google StreetView

53. After thoroughly reviewing the existing record in this investigation and applicable law, the Bureau has decided not to take enforcement action against Google for violation of Section 705(a). There is no Commission precedent addressing the application of Section 705(a) in connection with Wi-Fi communications. The available evidence, moreover, suggests that Google collected payload data only from unencrypted Wi-Fi networks, not from encrypted ones.[174] Google argues that the Wiretap Act permits the interception of unencrypted Wi-Fi communications, and some case law suggests that Section 705(a)'s prohibition on the interception or unauthorized reception of interstate radio communications excludes conduct permitted (if not expressly authorized) under the Wiretap Act.[175] Although Google also collected and stored encrypted communications sent over unencrypted Wi-Fi networks,[176] the Bureau has found no evidence that Google accessed or did anything with such encrypted communications. The Bureau's inability to compel an interview of Engineer Doe made it impossible to determine in the course of our investigation whether Google did make any use of any encrypted communications that it collected. For all these reasons, we do not find sufficient evidence that Google has violated Section 705(a) to support a finding of apparent liability under that provision in the context of this case.

Conclusion

- FCC enforcement is driven by complaints and prioritization
  - life safety, commercial TV & radio, cellular
- Direction finder model does not scale
  - particularly with reduced field staff
- Automating enforcement has been discussed, but difficult
  - mobile, short range, intermittent
  - non-traditional emitters (LEDs, BitCoin mining)
- Wireless intercept rules lack clarity
  - intent, encryption, usage, bands (satellite, cellular)
  - but relatively clear for interference mitigation

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov