

In the
United States Court of Appeals
For the Seventh Circuit

No. 04-2328

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

RAJIB K. MITRA,

Defendant-Appellant.

Appeal from the United States District Court
for the Western District of Wisconsin.
No. 03-CR-153-S—**John C. Shabaz**, *Judge*.

ARGUED FEBRUARY 16, 2005—DECIDED APRIL 18, 2005

Before EASTERBROOK, WOOD, and SYKES, *Circuit Judges*.

EASTERBROOK, *Circuit Judge*. Wisconsin's capital city uses a computer-based radio system for police, fire, ambulance, and other emergency communications. The Smartnet II, made by Motorola, spreads traffic across 20 frequencies. One is designated for control. A radio unit (mobile or base) uses the control channel to initiate a conversation. Computer hardware and software assigns the conversation to an open channel, and it can link multiple roaming units into "talk groups" so that officers in the field can hold joint conversations. This is known as a "trunking system" and

makes efficient use of radio spectrum, so that 20 channels can support hundreds of users. If the control channel is interfered with, however, remote units will show the message “no system” and communication will be impossible.

Between January and August 2003 mobile units in Madison encountered occasional puzzling “no signal” conditions. On Halloween of that year the “no system” condition spread citywide; a powerful signal had blanketed all of the City’s communications towers and prevented the computer from receiving, on the control channel, data essential to parcel traffic among the other 19 channels. Madison was hosting between 50,000 and 100,000 visitors that day. When disturbances erupted, public safety departments were unable to coordinate their activities because the radio system was down. Although the City repeatedly switched the control channel for the Smartnet system, a step that temporarily restored service, the interfering signal changed channels too and again blocked the system’s use. On November 11, 2003, the attacker changed tactics. Instead of blocking the system’s use, he sent signals directing the Smartnet base station to keep channels open, and at the end of each communication the attacker appended a sound, such as a woman’s sexual moan.

By then the City had used radio direction finders to pin down the source of the intruding signals. Police arrested Rajib Mitra, a student in the University of Wisconsin’s graduate business school. They found the radio hardware and computer gear that he had used to monitor communications over the Smartnet system, analyze how it operated, and send the signals that took control of the system. Mitra, who in 2000 had received a B.S. in computer science from the University, possessed two other credentials for this kind of work: criminal convictions (in 1996 and 1998) for hacking into computers in order to perform malicious mischief. A jury convicted Mitra of two counts of intentional interference with computer-related systems used in interstate

commerce. See 18 U.S.C. §1030(a)(5). He has been sentenced to 96 months' imprisonment. On appeal he says that his conduct does not violate §1030—and that, if it does, the statute exceeds Congress's commerce power.

Section 1030(a)(5) provides that whoever

(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

- (iv) a threat to public health or safety; or
- (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security . . .

shall be punished as provided in subsection (c) of this section.

Subsection (e)(1) defines “computer” as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device”. Subsection (e)(2)(B) defines a “protected computer” to include any computer “used in interstate or foreign commerce or communication”. Finally, subsection (e)(8) defines “damage” to mean “any impairment to the integrity or availability of data, a program, a system, or information”.

The prosecutor’s theory is that Smartnet II is a “computer” because it contains a chip that performs high-speed processing in response to signals received on the control channel, and as a whole is a “communications facility directly related to or operating in conjunction” with that computer chip. It is a “protected computer” because it is used in “interstate . . . communication”; the frequencies it uses have been allocated by the Federal Communications Commission for police, fire, and other public-health services. Mitra’s transmissions on Halloween included “information” that was received by the Smartnet. Data that Mitra sent interfered with the way the computer allocated communications to the other 19 channels and stopped the flow of information among public-safety officers. This led to “damage” by causing a “no system” condition citywide,

impairing the “availability of . . . a system, or information” and creating “a threat to public health or safety” by knocking out police, fire, and emergency communications. See §1030(a)(5)(A)(i), (B)(iv). The extraneous sounds tacked onto conversations on November 11 also are “information” sent to the “protected computer,” and produce “damage” because they impair the “integrity” of the official communications. This time subsection §1030(a)(5)(B)(v) is what makes the meddling a crime, because Mitra hacked into a governmental safety-related communications system.

Mitra concedes that he is guilty if the statute is parsed as we have done. But he submits that Congress could not have intended the statute to work this way. Mitra did not invade a bank’s system to steal financial information, or erase data on an ex-employer’s system, see *United States v. Lloyd*, 269 F.3d 228 (3d Cir. 2001), or plaster a corporation’s web site with obscenities that drove away customers, or unleash a worm that slowed and crashed computers across the world, see *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), or break into military computers to scramble a flight of interceptors to meet a nonexistent threat, or plant covert programs in computers so that they would send spam without the owners’ knowledge. All he did was gum up a radio system. Surely that cannot be a federal crime, Mitra insists, even if the radio system contains a computer. Every cell phone and cell tower is a “computer” under this statute’s definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget. Reading §1030 to cover all of these, and police radio too, would give the statute wide coverage, which by Mitra’s lights means that Congress cannot have contemplated such breadth.

Well of course Congress did not contemplate or intend this particular application of the statute. Congress is a “they” and not an “it”; a committee lacks a brain (or, rather, has so many brains with so many different objectives that it is

almost facetious to impute a joint goal or purpose to the collectivity). See Kenneth A. Shepsle, *Congress is a “They,” Not an “It”: Legislative Intent as Oxymoron*, 12 Int’l Rev. L. & Econ. 239 (1992). Legislation is an objective text approved in constitutionally prescribed ways; its scope is not limited by the cerebrations of those voted for or signed it into law.

Electronics and communications change rapidly, while each legislator’s imagination is limited. Trunking communications systems came to market after 1984, when the first version of §1030 was enacted, and none of the many amendments to this statute directly addresses them. But although legislators may not know about trunking communications systems, they *do* know that complexity is endemic in the modern world and that each passing year sees new developments. That’s why they write general statutes rather than enacting a list of particular forbidden acts. And it is the statutes they enacted—not the thoughts they did or didn’t have—that courts must apply. What Congress would have done about trunking systems, had they been present to the mind of any Senator or Representative, is neither here nor there. See *West Virginia University Hospitals, Inc. v. Casey*, 499 U.S. 83, 100-01 (1991).

Section 1030 is general. Exclusions show just *how* general. Subsection (e)(1) carves out automatic typewriters, typesetters, and handheld calculators; this shows that other devices with embedded processors and software are covered. As more devices come to have built-in intelligence, the effective scope of the statute grows. This might prompt Congress to amend the statute but does not authorize the judiciary to give the existing version less coverage than its language portends. See *National Broiler Marketing Ass’n v. United States*, 436 U.S. 816 (1978). What protects people who accidentally erase songs on an iPod, trip over (and thus disable) a wireless base station, or rear-end a car and set off a computerized airbag, is not judicial creativity but the

requirements of the statute itself: the damage must be intentional, it must be substantial (at least \$5,000 or bodily injury or danger to public safety), and the computer must operate in interstate or foreign commerce.

Let us turn, then, to the commerce requirement. The system operated on spectrum licensed by the FCC. It met the statutory definition because the interference affected “communication.” Mitra observes that his interference did not affect any radio system on the other side of a state line, yet this is true of many cell-phone calls, all of which are part of interstate commerce because the electromagnetic spectrum is securely within the federal regulatory domain. See, e.g., *Radovich v. National Football League*, 352 U.S. 445, 453 (1957); *Federal Radio Commission v. Nelson Brothers Bond & Mortgage Co.*, 289 U.S. 266, 279 (1933). Congress may regulate all channels of interstate commerce; the spectrum is one of them. See *United States v. Lopez*, 514 U.S. 549, 558 (1995); *United States v. Morrison*, 529 U.S. 598, 608-09 (2000). Mitra’s apparatus was more powerful than the Huygens probe that recently returned pictures and other data from Saturn’s moon Titan. Anyway, the statute does not ask whether the person who caused the damage acted in interstate commerce; it protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the *computer* is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire. (Indeed, Mitra concedes that he could have been prosecuted, consistent with the Constitution, for broadcasting an unauthorized signal. See 47 U.S.C. §301, §401(c).) Section 1030 is within the national power as applied to computer-based channel-switching communications systems.

Mitra offers a fallback argument that application of §1030 to his activities is so unexpected that it offends the due process clause. But what cases such as *Bouie v. Columbia*,

378 U.S. 347 (1964), hold is that a court may not apply a clear criminal statute in a way that a reader could not anticipate, or put a vague criminal statute to a new and unexpected use. Mitra's problem is not that §1030 has been turned in a direction that would have surprised reasonable people; it is that a broad statute has been applied *exactly as written*, while he wishes that it had not been. There is no constitutional obstacle to enforcing broad but clear statutes. See *Rogers v. Tennessee*, 532 U.S. 451, 458-62 (2001) (discussing *Bouie*'s rationale and limits). The statute itself gives all the notice that the Constitution requires.

During deliberations the jury inquired about the meaning of the word "intentionally." The judge referred them to the instructions, which included a definition. Mitra says that the judge should have drafted a new definition, because the first must have been confusing (though he concedes that it was correct). This sort of problem is one for the district judge to resolve on the spot; there would be little point in Monday morning quarterbacking.

Sentencing requires but little discussion. The district judge added offense levels under U.S.S.G. §2B1.1(b)(13)(A)(iii) and (B) after concluding that Mitra had disrupted a "critical infrastructure". (Our citations are to the 2003 Manual, which the district judge used; the current version is substantively identical but numbered a little differently.) Application Note 12 defines that term; Mitra concedes that an emergency radio system fits the definition. Emergency services are one of the note's examples. Once again his argument takes the form that the authors of this language just couldn't have meant what they said. It is not as if the note were a linguistic garble, or that it is impossible to fathom why any sane person would think that the penalty for crippling an emergency-communication system on which lives may depend should be higher than the penalty for hacking into a web site to leave a rude message. The district judge was right to apply the guideline and note as written.

Mitra was sentenced before *United States v. Booker*, 125 S. Ct. 738 (2005), and did not argue in the district court that the sixth amendment limits the judge's role in sentencing. Review now is limited to a search for plain error. The approach developed in *United States v. Paladino*, 401 F.3d 471 (7th Cir. 2005), applies to this sentence, which falls within a properly calculated guideline range. Accordingly, although the judgment of conviction is affirmed, we remand to the district court under the terms of *Paladino* so that the district judge may inform us whether the additional discretion provided by *Booker*'s remedial holding would affect Mitra's sentence.

A true Copy:

Teste:

*Clerk of the United States Court of
Appeals for the Seventh Circuit*