Should Satellite Pirates Walk the Plank? Navigating the High Seas of the Federal Wiretap Act

Robert B. Preston*

I. INTRODUCTION

Direct Broadcast Satellite (DBS) is a technology that transmits digitalized audio and video signals to homes and businesses around the world via a network of orbital satellites. DBS providers generate revenue by charging viewers a monthly subscription fee for access to their systems. However, not all individuals who enjoy DBS programming compensate the providers for the service. Signal thieves, or pirates, use unauthorized devices to surreptitiously intercept and view the DBS providers' encrypted signals. Accordingly, DBS providers have initiated an aggressive campaign to plunder these pirates.

Through investigative efforts, DBS providers have procured evidence proving that some consumers have purchased pirate access equipment.[1] Under section 2512(1)(b) of the Wiretap Act,[2] as amended by the Electronic Communications Privacy Act of 1986 (ECPA),[3] possession of such equipment is illegal.[4] However, section 2520(a) provides that anyone whose "electronic communication is intercepted, disclosed, or intentionally used in violation of [the Wiretap Act] may in a civil action recover from the person . . . which engaged in that violation."[5] DBS providers argue that the conduct

* J.D. (2006), Washington University School of Law; B.S. *cum laude* (2003), Northwestern University.

1. *See* Sylvia Hsieh, *Direct TV Sues Consumers over Satellite Signal Theft*, LAW WKLY. USA, June 23, 2003, at 15.

2. 18 U.S.C. §§ 2510–20 (2000).

3. Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.).

4. 18 U.S.C. § 2512(1)(b).

5. *Id.* § 2520(a); *see infra* notes 46–48 and accompanying text.

specified in section 2512(1)(b) is encompassed by section 2520(a) because of the phrase, "in violation of [the Wiretap Act]."[6] A minority of courts that have considered this issue have been persuaded by this logic. Alleged pirates argue, and a majority of courts have held, that section 2520(a) does not provide a private cause of action against the mere possession of such equipment.

Accordingly, this Note focuses on this conflict and the arguments put forth by each side to buttress their respective positions. Part II begins by tracing the events that instigated this debate. Part II also discusses the statutory framework at the heart of this dispute, and outlines the divergent bodies of case law. Part III dissects the arguments advanced by each side, and considers the merits of each in light of common canons of statutory interpretation. Finally, Part IV concludes that the majority position is correct.

II. CONGRESS, COMMUNICATIONS, AND THE COURTS

A. Background

To view DBS programming, viewers must acquire a fixed outdoor satellite dish.[7] The dish transmits signals to an indoor receiver that feeds them into a television monitor.[8] DirecTV, the nation's leading DBS provider, claims that it has invested more than $1.25 billion in the development of its system.[9]

To protect their investments, DBS providers digitally encrypt, or scramble, their signals to prevent unauthorized access.[10] Typically, indoor receivers feature a removable access card that contains the information necessary to decrypt, or unscramble, the signals.[11] Consumers pay an average of $61 per month for access to these services.[12]

---

6. 18 U.S.C. § 2520(a).

7. *See* Peter Shinkle, *DirecTV Adopts Scorched-Earth Policy to Stop Pirates from Stealing Signals*, ST. LOUIS POST-DISPATCH, June 22, 2003.

8. *Id.*

9. Dan Christensen, *DirecTV Suing Customers Directly*, MIAMI DAILY BUS. REV., June 17, 2003.

10. *See, e.g.*, DirecTV, Inc. v. Treworgy, 373 F.3d 1124, 1125 (11th Cir. 2004).

11. *Id.*; *see also* Hsieh, *supra* note 1, at 15.

12. Kevin Poulsen, *DirecTV Dragnet Snares Innocent Techies*, SECURITYFOCUS, July 17,

However, individuals have developed various pirate access devices capable of unscrambling the signals without the authorization of or payment to the DBS providers.[13] Of the two DBS providers in the United States, DirecTV and Dish Network, DirecTV has been hardest hit.[14] Unauthorized viewing, or "pirating," costs DirecTV an estimated $1.2 billion each year.[15] Accordingly, DirecTV has spent considerable resources to combat what essentially constitutes theft of its product. In the early stages of this effort, DirecTV targeted the producers, marketers and sellers of pirate access devices.[16] Through investigation of these providers, DirecTV obtained information suggesting that tens of thousands of consumers purchased pirate access devices.[17] DirecTV then initiated two programs, the "End User

---

2003, http://www.securityfocus.com/news/6402.

13. The struggle between DBS providers and the producers of pirate access devices is a colorful game of cat and mouse. The original devices were little more than preprogrammed access cards that enabled viewers to decrypt DBS signals. DirecTV, Inc. v. Little, No. CV-03-2407 RMW, 2004 U.S. Dist. LEXIS 16350, at *2 (N.D. Cal. Aug. 12, 2004). Thereafter, pirates began to use access card rewriters to continually update their cards. *Id.* Whenever the DBS providers updated their encryption technologies, hackers would publish the new codes on their websites, and viewers simply reformatted their cards using the rewriters. *See* Dorothy Pomerantz, *Stealing the Show*, FORBES.COM, May 29, 2003, http://www.forbes.com/2003/05/29/cz_dp_0529directv.html. In order to combat the theft of their product, DBS providers occasionally implement electronic countermeasures (ECMs), which are signals that target and disable illegally modified access cards by reprogramming the cards to run in an endless loop. *Little*, 2004 U.S. Dist. LEXIS at *4. To combat this problem, pirates created devices, dubbed "unloopers," to reprogram the cards to their previous configuration. *Id.*; *see also* Arik Hesseldahl, *TV Pirates Smacked down*, FORBES.COM, Jan. 29, 2001, http://www.forbes.com/2001/01/29/0129directv.html.

14. In 2003, The Carmel Group, a satellite consulting firm, estimated that "2.2 million Americans [would] steal satellite service from . . . DirecTV compared with 720,000 from DirectTV rival Echostar." Pomerantz, *supra* note 13. The Carmel Group estimates that the number of pirates stealing DirecTV's service could inflate to 3.3 million by 2006. *Id.* Piracy is more of a problem for DirecTV than its rival because its system is easier to hack. *Id.*

15. *Id.*

16. Shinkle, *supra* note 7. Additionally, DirecTV has sought to shut down websites devoted to DBS theft. On April 30, 2003, a Florida judge granted a restraining order shutting down sixty-three web sites. Pomerantz, *supra* note 13. The largest of these sites, "Decoder News," had more than 23,000 paying subscribers. Christensen, *supra* note 9. DirecTV claims that it intends to pursue those who frequented these sites. *Id.*

17. "In some cases, DirectTV used federal civil forfeiture laws under the Digital Millennium Copyright Act to get local police to raid companies that sell pirating equipment." Hsieh, *supra* note 1, at 15.

For instance, in 2001, federal investigators raided Fulfillment Plus, a mailing facility used by various mail order and internet retailers to facilitate their businesses. DirecTV, Inc. v. Treworgy, 373 F.3d 1124, 1125 (11th Cir. 2004). DirecTV executed writs of seizure at

Discovery Group" and the "End User Recovery Project," to mitigate signal theft by going after these consumers directly.[18]

Armed with this information, DirecTV's end user groups commenced a second, more controversial assault. DirecTV sent demand letters to all consumers linked with the purchase of a pirate access device.[19] These letters listed a number of federal statutes that deal with the interception of electronic signals.[20] Recipients were

---

Fulfillment Plus. *Id.* Through the ensuing investigation, DirecTV secured hundreds of sales records and credit card receipts evidencing the purchase of pirate access devices. *Id.* This raid gave rise to a number of cases, including *DirecTV, Inc. v. Cardona*, 275 F. Supp. 2d 1357 (M.D. Fla. 2003), and *DirecTV, Inc. v. Drury*, 282 F. Supp. 2d 1321 (M.D. Fla. 2003).

18. Hsieh, *supra* note 1, at 15.

19. In 2002 and 2003, DirecTV sent out more than 100,000 letters. *Id.*

20. One such letter, dated June 13, 2003, provides:

> The DIRECTV End User Development Organization is responsible for the investigation of individuals receiving DIRECTV programming without authorization. Illegal reception and use of DIRECTV is accomplished through the use of modified DIRECTV Access Cards (sometimes referred to as "test cards") and other illegal signal theft devices.
>
> Business records recently obtained by this office show that you purchased illegal signal theft equipment to gain unauthorized access to DIRECTV programming. We are contacting you because your purchase and use, or attempted use, of illegal signal theft equipment to access DIRECTV programming violates federal and state laws.
>
> Federal and state statutes impose serious civil damages against those who possess and use illegal theft equipment. *See* 47 U.S.C. § 605(a) (making it illegal to receive assist another in receiving an encrypted satellite signal); 18 U.S.C. § 2511(1)(a)(making it illegal to intercept an encrypted satellite signal); 17 U.S.C. § 1201(a)(1)(making it illegal to circumvent a technological measure such as DIRECTV conditional access system). So strict are these statutes that Congress has made the **mere possession** of signal theft equipment a violation of federal law in certain circumstances. *See* 18 U.S.C. § 2512(1)(b)(making it illegal to "possess" an electronic, mechanical or other device sent by mail, knowing or having reason to know that the design of the devise renders it primarily useful for the surreptitious interception of an encrypted satellite signal).
>
> Your purchase, possession and use of the signal theft equipment to gain unauthorized access to DIRECTV's satellite television programming subjects you to statutory damages of up to $10,000 **per violation**. *See* 47 U.S.C. § 605(e)(3). Moreover, your involvement in modifying devices to illegally gain access to DIRECTV's programming increases potential statutory damages to $100,000. Finally, these statutes allow DIRECTV to recover from you compensatory and punitive damages, attorneys' fees and other expenses. *See* 47 U.S.C. § 605(c)(3)(B); 18 U.S.C. § 2520(b). Thus, individuals in any way involved with illegal signal theft equipment face substantial monetary damage awards for their conduct.
>
> DIRECTV is making this offer to rectify past misappropriations of its satellite programming by users of signal theft equipment and to prevent the use of illegal

instructed to contact DirecTV or face litigation and damages of $100,000 or more.[21] As to those who opted to settle, DirecTV demanded that the alleged pirate surrender all illegal devices, vow never to buy them again, and pay damages of approximately $3500.[22]

> access devices in the future. Satellite piracy is illegal and results in unfair expense to DIRECTV and its paying subscribers. For this reason, DIRECTV actively pursues legal action against those engaged in signal theft.
>
> With the above goals in mind and in light of DIRECTV's signal theft claims against you, we would like to resolve this matter with you. In return for your cooperation, DIRECTV is willing to forego its claims against you for violations accruing prior to the date of this letter. DIRECTV is prepared to release its claim in return for your agreement to: (1) surrender all illegally modified Access Cards or other satellite signal theft devices in your possession, custody or control; (2) execute a written statement to the effect that you will not purchase or use illegal signal theft devices to obtain satellite programming in the future, nor will you have any involvement in the unauthorized reception and use of DIRECTV's satellite television programming; and (3) pay a monetary sum to DIRECTV for your past wrongful conduct and the damages thereby incurred by the company.
>
> If you should choose to reject DIRECTV's settlement offer, or should you fail to respond, please be advised that DIRECTV will take all measures to preserve its rights and remedies under federal and state law. This may involve the initiation of legal proceedings in Federal District Court seeking the award of damages and other relief discussed above.
>
> While we are willing to discuss this matter with you, DIRECTV will not imprudently and indefinitely wait for you to acknowledge your unlawful conduct. **Therefore, to discuss the contents of this letter, you must contact an investigator at [redacted] on or before 6:00 p.m., Pacific Standard Time, June 27, 2003. Any available Investigator can handle your call.** Please reference your case number . . . when you call. After that date, DIRECTV will abandon its attempts to negotiate and/or amicably resolve this matter. In any event, as a result of this investigation, DIERCTV Customer Service representatives will not be able handle questions regarding your illegal access to DIRECTV satellite programming. **Please direct any and all future inquiries to this office.**
>
> There is little question that you will benefit by resolving this matter through informal discussion. Illegal access to DIRECTV programming is a serious problem and, consequently, DIRECTV has no choice but to fully pursue illegal residential access cases to the end. . .

Letter from DirecTV to Customer, June 13, 2003, *available at* http://www.directvdefense.org/files/letter2.pdf. Additional sample letters are available at http://www.directvdefense.org/files/letter1.pdf (last visited May 16, 2006); http://www.overhauser.com/DTV/Articles/Secure%20Letters%20I.pdf (last visited May 16, 2006); http://www.overhauser.com/DTV/Articles/Secure%20Letters%20II.pdf (last visited May 16, 2006).

21. *Id.*

22. *Id.*; *see also* Christensen, *supra* note 9.

Because satellite signal interception is a passive process, DirecTV cannot determine if pirates are actually using the devices to intercept their signals. A consumer's purchase of a pirate access device is the only evidence of pirating available to DirectTV. Nevertheless, as of the end of June, 2003, DirecTV sent more than 100,000 demand letters and filed more than 8700 lawsuits around the country.[23]

B. The Federal Wiretap Act[24]

In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act (OCCSSA).[25] Title III of the OCCSSA is commonly known as the "Wiretap Act." Section 2511(1) of the Wiretap Act provides that "any person who . . . uses . . . intercepts . . . [or] discloses . . . the contents of any wire, oral, or electronic

23. Hsieh, *supra* note 1, at 15.

24. 18 U.S.C. §§ 2510–20. The Wiretap Act is not the only statute used to prosecute pirates. Section 705 of the Communications Act of 1934, 47 U.S.C. §§ 605(a), (e)(4) (2000), as amended by the Cable Communications Policy Act of 1984 (CCPA), Pub. L. No. 98–549, 98 Stat. 2779 (1984), and the Satellite Home Viewer Act of 1988 (SHVA), Pub. L. No. 100–667, 102 Stat. 3949 (1988), prescribes criminal penalties for anyone who intentionally intercepts or aids in the interception of commercial communications. This statute provides, in pertinent part, that "[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." 47 U.S.C. § 605(a). Section 605(e)(4) extends liability to "[a]ny person who manufactures, . . . sells, or distributes any . . . device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of [satellite television signals]." *Id.* § 605(e)(4).

The clear meaning of these statutes sharply delineates the activity that is prohibited by the law. Purchase and possession are conspicuously absent. Accordingly, numerous courts have confirmed that these statutes do not prohibit mere purchase or possession of pirate access devices. *See, e.g.*, Smith v. Cincinnati Post & Times-Star, 475 F.2d 740 (6th Cir. 1973); V Cable, Inc. v. Guercio, 148 F. Supp. 2d 236 (E.D.N.Y. 2001).

Another statute often invoked in satellite piracy cases is the Digital Millennium Copyright Act (DMCA). 17 U.S.C. § 1201(a)(1)(A) (2000). This Act provides, in pertinent part, that "no person shall circumvent a technological measure that effectively controls access to a work protected by [the DCMA]." *Id.* Accordingly, the plain language of the Act clearly prohibits only the act of circumvention, not purchase or possession.

The foregoing statutes are quite effective when DirecTV has evidence that its signals were actually intercepted. In most cases, however, DirecTV has no such evidence. Moreover, the Wiretap Act arguably provides for a private cause of action.

25. Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended in scattered sections of 18 U.S.C.). Title III was essentially a combination of the Federal Wire Interception Act and the Electronic Surveillance Control Act of 1967. S. REP. NO. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)."[26]

Prior to 1986, section 2512 provided:

> [A]ny person who willfully. . . . possesses, or sells any . . . device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral wire communications . . . shall be fined not more than $10,000 or imprisoned not more than five years, or both.[27]

In addition, section 2520 provided that "[a]ny person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses . . . such communications, and (2) be entitled to recover [damages and attorney's fees] from any such person."[28]

DBS providers argue that the phrase "in violation of this chapter" provides a private right of action under section 2520 against the possession of a pirate access device, conduct that is criminalized in section 2512. This argument was first asserted by the plaintiff in *Flowers v. Tandy Corp.*[29]

---

26. "[W]hoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." 18 U.S.C. § 2511(4)(a). "[T]he person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction." *Id.* § 2511(5)(a)(i).

27. 18 U.S.C. § 2512 (1968).

28. 18 U.S.C. § 2520 (2000) (as amended by Pub. L. No. 91-358, tit. II, § 211(c), 84 Stat. 473 (1970)). At the time that the Wiretap Act was enacted, this section read:

> Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—
>
> (a) actual damages . . .
>
> (b) punitive damages; and
>
> (c) a reasonable attorney's fee and other litigation costs reasonably incurred.

Id. § 2520 (1970).

29. 773 F.2d 585 (4th Cir. 1985).

C. The Seed of Conflict: Flowers v. Tandy Corp.

Flowers, the seminal case concerning the proper interpretation of section 2520, involved the Tandy Corporation ("Tandy"), which manufactured telephone recording devices, and William Flowers, who purchased a device to surreptitiously record telephone conversations between his wife and a suspected lover.[30] The co-plaintiffs filed a civil action against Tandy for aiding and abetting the illegal wiretapping by selling the device.[31] Though section 2520 only provided a civil right of action to persons "whose wire or oral communication is intercepted . . . or used in violation of this chapter,"[32] the co-plaintiffs argued that section 2512, which criminalized the possession or sale of such a device, could be used to determine whether Tandy was civilly liable under section 2520.[33] This argument was premised on an interpretation of section 2520 that presupposed that the phrase, "or used in violation of this chapter," encompassed conduct prohibited in section 2512.[34]

The jury found for the plaintiffs and awarded $60,000 in actual and $22,000 in punitive damages.[35] On appeal, the circuit court began its analysis by unequivocally stating that the "district court erred in permitting the jury to consider the criminal statute . . . as a basis for imposing civil liability."[36] In denying an encompassing reading of section 2520, Circuit Judge Phillips, writing for the court, noted that section 2520 closely tracks the language of section 2511.[37] As such, he reasoned that section 2520 was "not susceptible to a construction which would provide a cause of action against one who manufactures or sells a device in violation of § 2512 but does not engage in conduct violative of § 2511."[38]

---

30. *Id.* at 586.
31. *Id.* at 587.
32. 18 U.S.C. § 2520 (1970). For the full text of the statute as it existed at the time of the case, see *supra* note 28 and accompanying text.
33. *Flowers*, 773 F.2d at 587.
34. *Id.* at 588.
35. *Id.*
36. *Id.*
37. *Id.* at 588–89.
38. *Id.* The specific language the court rejected as providing a private cause of action for violations of section 2512 provided that a party would have a private cause of action "against

This conclusion is supported by the general theory that "implied causes of action are disfavored and should be found only where a statute clearly indicates that the plaintiff is one of a class for whose benefit the statute was enacted."[39] Congress enacted section 2512, a criminal statute, to benefit society as a whole by ridding the market of pirate devices.[40] It enacted section 2520, on the other hand, to protect the specific victims of illegal interception.[41]

Following *Flowers*, few courts considered the circumstances necessary for a plaintiff to file a private cause of action under section 2520. However, as telecommunications technology became more sophisticated, Congress realized that the Wiretap Act needed to be amended to stay germane.[42]

D. The ECPA

Nearly twenty years after the Wiretap Act's enactment, Senators Leahy (D-VT) and Mathias (R-MD) introduced the ECPA to the Senate.[43] Senator Leahy noted that the Wiretap Act of 1968 was "hopelessly out of date."[44] In response, Congress enacted the ECPA, which was the first major revision of the Wiretap Act. Little has changed in the relevant sections of the Wiretap Act since the ECPA's passage.

---

any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications." *Id.* at 587 n.2.

39. *Id.* at 589 (citing Cort v. Ash, 422 U.S. 66, 78 (1975)); *see also infra* note 151.

40. *Flowers*, 773 F.2d at 589; *see also* Cox Cable Cleveland Area, Inc. v. King, 582 F. Supp. 376 (N.D. Ohio 1983). In *Cox*, the court held, as matter of law, that section 2520 did not encompass action prohibited in section 2511(1)(a). *Id.* at 382. This decision was largely based on the legislative history of the Wiretap Act wherein Congress manifested its intent to protect only private communications from illegal wiretapping. *Id.*

41. *Flowers*, 773 F.2d at 589.

42. The Senate reported that the "bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunication technologies." S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

43. 132 CONG. REC. 14599 (1986).

44. *Id.* at 14600. The Senator elaborated that "[e]ighteen years ago, Congress could not appreciate—or in some cases even contemplate—[today's] telecommunications and computer technology." *Id.*

In section 2512(1)(b), the ECPA substituted the word "intentionally" for "willfully."[45] The amendment also changed "wire or oral communication" to "wire, oral, or *electronic communication*" in five locations.[46] The ECPA also largely rewrote section 2520.[47] The amended statute read, in relevant part, that, "except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate."[48]

---

45. S. REP. NO. 99-541 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

46. Pub. L. No. 99-508, § 101(c)(1)(A), 100 Stat. 1848 (1986) *(*emphasis added). After the enactment of the ECPA, section 2512 provided:

> Except as otherwise specifically provided in this chapter, any person who intentionally—
>
> . . . .
>
> (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications . . . or
>
> (c) places in any newspaper, magazine, handbill, or other publication any advertisement of—
>
> (i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
>
> (ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

18 U.S.C. § 2512.

47. For the full text of the statute prior to the 1986 amendments, see *supra* note 28 and accompanying text.

48. Section 2511(2)(a)(ii) provides:

> Notwithstanding any other law, providers of wire or electronic communication service . . . are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance . . . if such provider . . . has been provided with—
>
> (A) a court order directing such assistance signed by the authorizing judge, or
>
> (B) a certification in writing . . . that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required
>
> . . . .

18 U.S.C. § 2511(2)(a)(ii).

E. What Is a Device Primarily Useful for the Surreptitious Interception of Electronic Communication?

The minority's argument presumes that individuals in possession of a pirate access device act in violation of section 2512(1)(b). However, some courts have been unwilling to accept this presumption. The ECPA amended section 2512 to impose criminal liability on anyone who "possesses[] or sells any . . . device, knowing . . . that the design of such device renders it primarily useful for the purpose of the surreptitious interception . . . electronic communications."[49] In the early 1990s, a series of criminal cases at the circuit level attempted to discern whether pirate access devices were "primarily useful for the purpose of the surreptitious interception of . . . electronic communications."[50]

In *United States v. Herring*,[51] the Eleventh Circuit held that the ECPA regulated only private, or point-to-point, communications.[52] The court emphasized that the legislative history of the ECPA suggests that the Communications Act alone protects DBS signals.[53] However, in *United States v. McNutt*,[54] the Tenth Circuit gave the ECPA a much broader application. In *McNutt*, the court stated that the "plain wording of [the ECPA] encompasses satellite television signals."[55]

Although the Eleventh Circuit provided a far more thorough analysis than the Tenth with regard to the meaning of "electronic communications" as used in the ECPA, it erroneously reasoned that Congress would not enact two laws, the Communications Act and the

---

49. *Id.* § 2512; *see also supra* note 46.

50. *See* Samuel Rosenstein, Note, *The Electronic Communications Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolescence*, 76 MINN. L. REV. 1451, 1452–53 n.13 (1992) (listing cases).

51. 933 F.2d 932 (11th Cir. 1991).

52. *Id.* at 938; *see also* United States v. Hux, 940 F.2d 314, 318 (8th Cir. 1991) (adopting the Eleventh Circuit's interpretation).

53. *Herring*, 933 F.2d at 937–38. The Senate report relied on most heavily by the court read: "The private viewing of satellite cable programming . . . will continue to be governed exclusively by . . . the Communications Act . . . and not by [the ECPA]." S. REP. NO. 99-541, *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3576. For a discussion of the Communications Act, see *supra* note 24.

54. 908 F.2d 561 (10th Cir. 1990).

55. *Id.* at 564.

ECPA, to govern the same thing.[56] Not only is there patent evidence on the face of the statute and in the legislative history[57] of the ECPA suggesting that the Act is meant to govern satellite communications, but the legislative history of the Satellite Home Viewers Act of 1988 (SHVA), a 1988 amendment to the Communications Act, also indicated that the two acts are intended to overlap.[58]

Herring also touched upon a second issue as to whether a device is primarily useful for the surreptitious interception of electronic communications. Namely, the Eleventh Circuit considered whether the technology used to intercept the signals could also be used for other purposes.[59] On this point, the Senate noted that "[a] device will not escape the prohibition merely because it may have innocent uses. The crucial test is whether the design of the device renders it *primarily* useful for *surreptitious* listening."[60] In *Herring*, the court ruled that the devices at bar were no different in design than other, legitimate descramblers, and therefore that section 2512(b)(1) did not apply.[61]

DirecTV, Inc. v. Little[62] provides a vivid example of this debate as it exists today. In *Little*, the defendant operated "Techs on Call," a

---

56. *Herring*, 933 F.2d at 938.

57. Section 2510(12) of the Wiretap Act indicates that "electronic communications" includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce."

58. Section "2511(1) [of the ECPA] . . . prohibit[s] the unauthorized interception and use of satellite [television]." H.R. REP. NO. 100-887(II) (1988), *as reprinted in* 1988 U.S.C.C.A.N. 5638, 5643 (1988). For a discussion of the SHVA, see *supra* note 24.

59. *Herring*, 933 F.2d at 933–34.

60. S. REP. NO. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2183.

61. *Herring*, 933 F.2d at 934. Through expert testimony, the court found:

> [S]oftware built into the descramblers was seventy-five percent identical to that in authorized descrambler units . . . Because the design of the descramblers gives them significant nonsurreptitious and legitimate uses, and therefore the descramblers are not primarily useful for surreptitious listening, there is no possibility that appellants could have been convicted under section 2512(1)(b) prior to 1986.

Id.; *see also* United States v. Schweihs, 569 F.2d 965, 968 (5th Cir. 1978) (finding that a device constructed or purchased specifically for use in covert wiretapping or eavesdropping is not prohibited by section 2512 if its design characteristics do not render it primarily useful for that purpose).

62. No. CV-03-2407 RMW, 2004 U.S. Dist. LEXIS 16350 (N.D. Cal. Aug. 12, 2004).

small computer repair and network consulting company.[63] As part of his business, the defendant purchased forty-six reader/writers from a distributor of pirate access devices.[64] DirecTV, however, claimed that this equipment "was designed for the purpose of circumventing DirecTV's conditional access controls."[65] DirecTV also underscored the fact that the equipment was specifically marketed as a pirate access device, not as a programmable access card appropriate for legal uses.[66] Finally, DirecTV claimed that the defendant purchased additional software from other websites devoted to pirating satellite signals.[67] Despite this evidence, the court stated that it could not rule as a matter of law that the reader/writer was designed primarily for illegal purposes.[68]

Despite *Little*, modern courts are likely to accept that a pirate access device is primarily useful for the surreptitious interception of electronic communications. This is evidenced by the fact that this issue is rarely contested at trial. Moreover, in *United States v. Lande*,[69] the Ninth Circuit held that "[s]atellite transmissions could not be intercepted any more 'surreptitious[ly]' than by these devices which cannot be detected by producers of electronic television programming."[70] The Ninth Circuit also held that the technical design of the device made it primarily useful for illegal purposes.[71]

---

63. *Id*. at *4–*5.

64. *Id.* at *7. The defense wrote a whitepaper detailing the steps by which the White Viper reader/writers could be used to implement a secured network access system. *Id.* at *12.

65. *Id.* at *8 (quoting an expert witness for DirecTV). The witness pointed to a number of features that indicated that the equipment was specially designed to serve an illegal purpose. Specifically, the witness asserted that the absence of a "card present" indicator on the reader/writer made it incompatible with Microsoft Windows. *Id.* at *10. Moreover, the unique layout of the reader/writer made it compatible with the unique layout of DirecTV access cards. *Id.*

66. *Id.* at *11.

67. *Id.* at *14.

68. *Id*. at *26.

69. 968 F.2d 907 (9th Cir. 1992).

70. *Id.* at 910; *see also* United States v. McNutt, 908 F.2d 561, 565 (10th Cir. 1990) (discussing the inherently surreptitious operations of a descrambler).

71. *Lande*, 968 F.2d at 910. The court stated: "It is difficult to imagine any purpose for these modified descramblers other than the unauthorized interception of satellite television signals. To be sure, before modification the descramblers might be put to legitimate use, but once modified they serve no purpose except to allow surreptitious interception." *Id.*

See United States v. Harrell, 983 F.2d 36 (5th Cir. 1993). In *Harrell*, the court found that a device that could legally be used to descramble DBS signals became a device primarily useful

Because of the ambiguous nature of the use of these cards, critics argue that DirecTV's indiscriminate campaign against all individuals who purchase pirate access devices is unethical—DirecTV not only snares signal pirates, but also innocent parties.[72] As such, critics argue that DirecTV is abusing the system by refusing to conduct a preliminary investigation prior to sending its demand letters.[73] Most of the individuals who receive the letters are either frightened and pay immediately, or find it cheaper to settle than to litigate the case.[74]

DirecTV maintains that its campaign is not as haphazard as its critics claim. DirecTV asserts that it only sues people who "bought devices clearly designed to steal TV programming"[75] from websites devoted to selling pirate access equipment.[76] Despite DirecTV's assertion of innocence, several defendants have filed counter-claims and pursued class action claims under state deceptive trade practices[77]

---

for the purpose of the surreptitious interception of wire, oral, or electronic communications when the seal on the device was broken and a programmed computer chip containing the address of a paying customer was inserted. *Id.* at 38. The court found it unreasonable to believe that an individual, having spent approximately $300 for this modified chip, would primarily limit him or herself to programming for which he or she paid. *Id*.; *see also* United States v. Davis, 978 F.2d 415, 419 (8th Cir. 1992) (holding that modifications to previously legal device rendered it suitable only for surreptitions use).

72. *See* Poulsen, *supra* note 12.

73. *Id.*

74. *Id.*

75. Hsieh, *supra* note 1, at 16 (quoting Christopher Murphy, DirecTV's assistant general counsel). Murphy elaborated, "[w]e're suing people who bought reader-writers plus something else, such as hardware or software that, when combined with a reader-writer, can be used to pirate a satellite signal. We're saying that anyone who bought a reader-writer plus something else cannot be using it for lawful purposes." *Id.*

However, critics retort that the devices sold on pirating websites have the same specifications as those on more reputable websites; the products on pirate sites, however, are generally less expensive. Poulsen, *supra* note 12. "If somebody is sophisticated enough to be pursuing programming smart cards, they're going to look at the specs of the device. They do not care how it is marketed; they're going to get the best deal." *Id*.

76. Poulsen, *supra* note 12. DirecTV spokesman, Robert Mercer, said, "how innocent is someone who goes to [a] website that is clearly identified as a pirate website that is devoted to selling equipment to steal satellite TV programming, and orders the equipment, knowing full well what they're getting? That's quite a stretch." *Id.*

77. One theory suggests that DirecTV's demand letters are unfair business practices because they assert that the consumer violated federal law even though DirecTV has no proof that the recipient actually intercepted the signal. Hsieh, *supra* note 1, at 15. In *DirecTV, Inc. v. Cephas*, 294 F. Supp. 2d 760 (M.D.N.C. 2003), a defendant brought a counterclaim against DirecTV asserting a violation of the North Carolina Unfair and Deceptive Trade Practices Act (UDTPA), N.C. GEN. STAT. § 75-1.1, which "prohibits the general use of unfair or deceptive

and Racketeer Influenced and Corrupt Organizations Act (RICO) statutes.[78]

F. Post-ECPA Case Law

1. The Minority

Oceanic Cablevision, Inc. v. M.D. Electronics[79] was the first major opinion to disagree with *Flowers*. Oceanic, the plaintiff, was a cable television provider that received programs from suppliers and retransmitted them to paying customers.[80] Like most cable systems, Oceanic offered various levels of service.[81] It transmitted premium channels in a scrambled form.[82] Only customers who paid for the premium channels received the equipment necessary to legally descramble the signals.[83] The defendant, however, developed and sold equipment capable of descrambling Oceanic's signals, which allowed purchasers to enjoy unlimited access to premium channels

---

practices in commerce." *Cephas*, 294 F. Supp. 2d at 765. The court refused to grant DirecTV's motion to dismiss the counterclaim, finding the defendant had sufficiently alleged that DirecTV had engaged in unfair practices by falsely accusing the defendants of a crime, representing that the distributor had the power of law enforcement, and threatening to take action not permitted by law. *Id.* at 766. *But see* DirecTV, Inc. v. Karpinsky, 269 F. Supp. 2d 918 (E.D. Mich. 2003). In *Karpinsky*, the defendant raised a number of counterclaims against DirecTV, including deceptive trade practices under the Michigan Consumer Protection Act. *Id.* at 928. However, the court ruled that because Karpinsky was not a subscriber to DirecTV's services, the two parties were not engaged in trade or commerce, as defined and required by the act. *Id.* As such, the statute was inapplicable. *Id.*

78. 18 U.S.C. §§ 1961–68 (2000). Under this statute, a plaintiff must show that: (1) the defendants committed two or more predicate offenses; (2) a RICO enterprise existed; (3) a nexus exists between the pattern of racketeering activity and the enterprise; and (4) an injury to the plaintiff's business or property by reason of the first three factors. *See* DirecTV, Inc. v. Rayborn, No. 5:03-CV-59, 2003 U.S. Dist. LEXIS 19680, at *7 (W.D. Mich. Oct. 20, 2003). In *Rayborn*, the court ruled in favor of DirecTV because the class' complaint did not allege two or more predicate offenses described in 18 U.S.C. § 1961(1), and because it did not allege injury to its businesses or properties. *Id.* at *7–8. Moreover, the court noted that "a threat of litigation if a party fails to fulfil [sic] even a fraudulent obligation does not constitute extortion, and is insufficient to support a RICO claim as a matter of law." *Id.* at *8 (citing *Karpinsky*, 269 F. Supp. 2d at 929–30).

79. 771 F. Supp. 1019 (D. Neb. 1991).

80. *Id.* at 1022.

81. *Id.*

82. *Id.*

83. *Id.*

without paying the monthly fee and without Oceanic's knowledge or consent.[84]

Among other claims,[85] Oceanic filed two claims premised on the amended Wiretap Act. Like the plaintiff in *Flowers*, Oceanic asserted that the sale of devices primarily useful for the surreptitious interception of electronic communications, criminalized in section 2512, created a private right of action under section 2520.[86] However, unlike *Flowers*, the court found in favor of Oceanic.[87]

In *Flowers*, the Fourth Circuit ruled that section 2520 did not provide a private cause of action for violations contained in section 2512.[88] However, Congress enacted the ECPA after the *Flowers* decision. Consequently, the *Oceanic* court focused on the amendments to determine whether *Flowers* was still good law.[89] First, the court considered section 103 of the ECPA, which essentially rewrote section 2520.[90] While the statute in effect at the time of *Flowers* provided that a cause of action would lie against "any person who intercepts, discloses, or uses, or *procures any other person to intercept, disclose or use such communications*,"[91] the amended statute provides that a person shall have a private right of action against any person who has "intercepted, disclosed or intentionally used, *in violation of this chapter*," the electronic communications of another.[92] In light of the statute's dramatically broadened scope, the court held that the plain language of section 2520 "confers a private cause of action upon persons when the action is brought against parties that have violated the provisions of §§ 2510–2521."[93]

---

84. *Id.*

85. Oceanic filed thirteen claims for relief, including two implicating the Wiretap Act. Of the remaining eleven, two were under RICO. *Id.* at 1022–24. Additionally, Oceanic filed a claim under the CCPA. *Id.* at 1024–25. The balance of the claims asserted various torts, including tortious interference with contractual relations, tortious interference with prospective advantage, tortious interference with lawful business, and unfair competition. *Id.* at 1029–30.

86. *Id.* at 1025–26.

87. *Id.* at 1029.

88. Flowers v. Tandy Corp., 773 F.2d 585, 589 (4th Cir. 1985).

89. *Oceanic*, 771 F. Supp. at 1027–28.

90. *Id.* at 1027.

91. 18 U.S.C. § 2520 (1970) (emphasis added).

92. *Id.* (2000) (emphasis added).

93. *Oceanic*, 771 F. Supp. at 1027; *see also* DirecTV, Inc. v. Drury, 282 F. Supp. 2d 1321

Subsequently, in *DirecTV, Inc. v. Perez*,[94] DirecTV filed suit against a consumer for using unauthorized devices to intercept its signals. In a brief opinion, the court accepted the reasoning of *Oceanic*.[95] Though the court conceded that this interpretation offers potential plaintiffs a broad ability to bring private rights of action, it posited that plaintiffs such as DirecTV have a strong incentive to protect their interests against unauthorized interception.[96] The court reasoned that coupling this incentive with the right to bring a private cause of action will "decrease[] the burden on already overextended federal prosecutors to pursue criminal convictions under this statute."[97] This rationale has been dubbed the "private attorney general" rationale.

Finally, in *Community Televisions Systems, Inc. v. Caruso*,[98] a cable system operator sued for theft of its services under the Communications Act of 1934.[99] Specifically, the defendants purchased devices that allowed them to view pay-per-view programming without paying.[100] The plaintiff's primary evidence was a receipt, confiscated from a dealer, indicating that the defendant purchased a pirate access device.[101] The district court ruled in favor of the plaintiff and awarded $10,000 in damages and attorney's

(M.D. Fla. 2003); DirecTV, Inc. v. Calamanco, No. 5:02-CV-4102-MWB, 2003 WL 21956187, at *2 (N.D. Iowa Jan. 21, 2003); DirecTV, Inc. v. EQ Stuff, Inc., 207 F. Supp. 2d 1077, 1084 (C.D. Cal. 2002). In *Drury*, the court noted that the statutory language that persuaded the Fourth Circuit in *Flowers* to rule in favor of the defendant was no longer present in the amended version of the statute. *Drury*, 282 F. Supp. 2d at 1323. Therefore, "[s]ection 2520 applies to all violations within Chapter 19 of Title 18 of the United States Code concerning 'Wire and Electronic Communications Interception and Interception of Oral Communications,' which includes 18 U.S.C. § 2512." *Id*. The court concluded that DirecTV's complaint "simply asserts a private cause of action that 18 U.S.C. § 2520(a) expressly authorizes for violations of 18 U.S.C. § 2512(1)(b)." *Id.*

94. 279 F. Supp. 2d 962 (N.D. Ill. 2003).
95. *Id.* at 964.
96. *Id.* at 964–65.
97. *Id.*
98. 284 F.3d 430 (2d Cir. 2002).
99. *Id.* at 432.
100. *Id.* at 433.
101. *Id.*

fees.[102] The Second Circuit affirmed, finding that the purchase of a pirate access device raises a "rebuttable presumption" of liability.[103]

2. The Majority

In light of this controversy, the Eleventh Circuit opted to weigh in on the issue. In *DirecTV, Inc. v. Treworgy*,[104] DirecTV acquired evidence through an investigation of a shipping facility that dealt with pirate access devices[105] that the defendant, Treworgy, had purchased such a device.

The district court granted Treworgy's partial motion to dismiss.[106] On appeal, the Eleventh Circuit affirmed.[107] It began its analysis with the plain meaning of the Wiretap Act.[108] First, the court established that sections 2520(a) and 2512(1)(b) deal with two distinct issues: section 2520(a) provides a civil remedy for the victim of a theft of electronic communications, while section 2512(1)(b) provides criminal punishment for those who steal electronic communications.[109] Because it provides a civil remedy, section 2520 defines both "victims for whose benefit the remedy exists and the offenders for whom liability is owed."[110] Specifically, the plaintiff is "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter."[111] The defendant, on the other hand, is "the person or entity which engaged *in that violation*."[112] Unlike the court in *Oceanic*,[113] the Eleventh Circuit construed the phrase, "in that violation," narrowly.[114] It held that the phrase "'which engaged *in that violation*' makes apparent the intent of Congress to limit liability to a certain

102. *Id.* at 434.
103. *Id.* at 436.
104. 373 F.3d 1124 (11th Cir. 2004).
105. *Id*. at 1125; *see also supra* note 17.
106. *Treworgy*, 373 F.3d at 1125.
107. *Id.*
108. *Id.* at 1126.
109. *Id*.
110. *Id.* at 1127.
111. *Id.* (citing 18 U.S.C. § 2520(a)).
112. *Id.* (citing 18 U.S.C. § 2520(a)).
113. *See supra* notes 69–92 and accompanying text.
114. *Treworgy*, 373 F.3d at 1127.

class of defendants. Congress chose to confine private civil actions to defendants who had 'intercepted, disclosed, or intentionally used [a communication] in violation of . . . [the Wiretap Act].'"[115]

In addition, the court articulated two policy considerations in support of its holding. First, the court contended that DirecTV's argument was constitutionally problematic.[116] For DirecTV to suffer harm from a pirate access device, a pirate must use the device to intercept DirecTV's signals.[117] Where, as here, DirecTV has evidence only that the defendant purchased a device, but no proof that the device was actually used to intercept its signals, DirecTV's evidence proves only a hypothetical harm.[118] Without a showing of actual harm, DirecTV cannot establish a "case or controversy," as required by the Constitution.[119]

Second, the court rejected the "private attorney general"[120] rationale set forth in *Perez*.[121] The court cited a 2001 Supreme Court opinion in which Justice Scalia, writing for the court, noted that "'courts may not create [a private right of action], no matter how desirable that might be as a policy matter, or how compatible with the statute,' because that is a determination Congress alone can make."[122]

---

115. *Id.* (internal citations omitted).

116. *Id.*

117. *Id.*

118. *Id.*; *see also* DirecTV v. Amato, 269 F. Supp. 2d 688, 691 (E.D. Va. 2003). In *Amato*, the court reasoned that "a plaintiff must allege the unlawful possession and use of eavesdropping equipment in order to maintain a cause of action under § 2511, but the mere possession of that equipment, alone, affords no civil recovery under either code section." *Id.*

119. *Treworgy*, 373 F.3d at 1127 (citing U.S. CONST. art. III, § 2). This section of the Constitution sets the metes and bounds of the judicial power of the federal courts. *See also* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (holding a conjectural or hypothetical injury insufficient to establish constitutional standing).

120. *Treworgy*, 373 F.3d at 1128–29.

121. DirecTV, Inc. v. Perez, 279 F. Supp. 2d 962, 964–65 (N.D. Ill. 2003).

122. *Treworgy*, 373 F.3d at 1128–29 (quoting Alexander v. Sandoval, 532 U.S. 275, 286–87 (2001)); *see also* DirecTV, Inc. v. Westendorf, No. 3:03cv50210, 2003 U.S. Dist. LEXIS 16236 (N.D. Ill. Sept. 15, 2003). In *Westendorf*, the court ruled that neither section 2520(a) nor section 2512(1)(b) gives rise to an implied cause of action. *Id.* at *3. Further, the court noted that Congress intended to create an express cause of action via section 2520(a). *Id.* at *4. When Congress provides an express cause of action, "an implied right of action is especially difficult to infer without powerful support in the legislative history." *Id.* (citations omitted). Finally, the court noted that there is nothing in the legislative history of the Wiretap Act or its amendments that suggests that Congress intended to create an implied cause of action. *Id.*

III. ANALYSIS

In *Treworgy*, the Eleventh Circuit stated that the issue at bar was "purely a matter of statutory interpretation."[123] In discerning the meaning of any statute, the initial inquiry should be limited to the language of the statute itself.[124] However, section 2520 is not the paradigm of a carefully drafted statute. As a result, courts have come to contradictory conclusions regarding its proper interpretation. Accordingly, an analysis of the Wiretap Act should not look simply at the language of the Act, but should also examine the legislative history of the ECPA and various public policy rationales.

A. The Four Corners of the Statute

As made obvious by the split in authority, the majority and the minority both have colorable arguments that the plain meaning of section 2520(a) supports their positions.[125] Specifically, the minority argues that the phrase "in violation of this chapter" refers to the entire Wiretap Act. Therefore, the mere possession of a pirate access device, criminalized in section 2512(1)(b), gives rise to a private cause of action.[126] The majority, on the other hand, avers that the phrase "in violation of this chapter" is a prepositional phrase that modifies the preceding terms "intercepted, disclosed, or intentionally used."[127] Thus, only interception, disclosure and intentional use serve as the basis for a private cause of action.

---

123. *Treworgy*, 373 F.3d at 1126.

124. The Eleventh Circuit, the same court that decided *Treworgy*, commented that "[w]hen the import of the words Congress has used is clear . . . we need not resort to legislative history, and we certainly should not do so to undermine the plain meaning of the statutory language." Harris v. Garner, 216 F.3d 970, 976 (11th Cir. 2000).

125. Both sides used common tools of statutory construction to construe the statute to support their side. However, numerous learned scholars have questioned the probative weights of the common canons. *See* Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are to Be Construed*, 3 VAND. L. REV. 395, 400–06 (1950).

126. *See, e.g.*, DirecTV, Inc. v. Drury, 282 F. Supp. 2d 1321, 1322–23 (M.D. Fla. 2003); *see also supra* note 93 and accompanying text.

127. *See Treworgy*, 373 F.3d at 1127. In *DirecTV, Inc. v. Bertram*, 296 F. Supp. 2d 1021 (D. Minn. 2003), the court explained that "as a matter of grammar and sentence structure, the phrase 'that violation' refers to the interception, disclosure, or intentional use of

Section 2520 provides that anyone who violates the Act is liable to the injured party, with the narrow exception of electronic communication service providers under section 2511(2)(a)(ii).[128] Under the rule of *exclusio unius est expressio alterius*, when one provision is specifically excluded, all others are presumed to be included.[129] Thus, because section 2520 excludes section 2511(2)(a)(ii), it is presumed to include all other sections. If Congress intended to circumscribe the scope of section 2520, it could have easily done so. Moreover, the legislative history of the ECPA is void of any suggestion that section 2512 should be excluded.[130]

The canon of construction known as *ejusdem generis*[131] supports the majority's position. This rule suggests that the specific actions enumerated in section 2520, interception and disclosure, limit the meaning of the phrase "used in violation of this chapter" to conduct that directly harms the plaintiff.[132]

---

communications mentioned earlier in the sentence" and not to the entire Wiretap Act. *Id.* at 1024.

128. 18 U.S.C. § 2520 (2000); *see supra* note 48 and accompanying text.

129. According to most federal courts, this maxim's more conventional twin, *expressio unius est exclusio alterius*, "is only a guide, whose fallibility can be shown by contrary indications that adopting a particular rule or statute was probably not meant to signal any exclusion of its common relatives." United States v. Vonn, 535 U.S. 55, 56 (2002). In reference to *exclusio unium est expressio alterius*, the maxim at issue, the Fourth Circuit noted, "[w]e think that this 'maxim' is even more tenuous than its opposite." Nelson v. Dalkon Shield Claimants Trust, No. 98-1080, 1998 U.S. App. LEXIS 21387, at *8 (4th Cir. Aug. 31, 1998).

130. In *Treworgy*, the Eleventh Circuit addressed this issue. 373 F.3d at 1127–28. Rather than considering the merits of the various canons of construction, the court looked to the language of the excluded section, section 2511(2)(a)(ii), to determine the reason for its exclusion. *Id.* This section excludes from liability any person or agency that assists law enforcement officers in wiretap activities. *Id.*; *see also* 18 U.S.C. § 2511(2)(a)(ii) (2000). The court believed that the contents of this exclusion "butresse[d] the conclusion that the liability created by section 2520(a) is confined to illegal interceptions, disclosures, and uses of electronic communications." *Treworgy*, 373 F.3d at 1127; *see also supra* notes 46–48 and accompanying text.

131. "A canon of construction that when a general word or phrase follows a list of specifics, the general word or phrase will be interpreted to include only items of the same type as those listed." BLACK'S LAW DICTIONARY 556 (8th ed. 2004).

132. *See, e.g.*, Heathman v. Giles, 374 P.2d 839 (Utah 1962). In *Heathman*, the lower court dismissed a plaintiff's tort claim against a prosecutor for failure to file a bond as required by state statute. *Id.* at 839. The statute required the filing of a bond in actions brought against "any sheriff, constable, peace officer, state road officer, or any other person charged with the duty of enforcement of the criminal laws." *Id.* The Utah Supreme Court reversed, reasoning that the officials specifically enumerated were all badge-carrying officers who provided the front line of law enforcement and who faced unique risks. *Id.* at 840. As such, the phrase "any other person

B. The Legislative History of the Wiretap Act

The crux of the minority's argument is the fact that the ECPA broadened the scope of the Wiretap Act beyond the Fourth Circuit's interpretation in *Flowers.* The minority argues that Congress' purpose in passing the ECPA was to create an effective mechanism for slowing the proliferation of unauthorized devices, which had become a significant problem since the passage of the Wiretap Act in 1968.[133] Indeed, Congress provided identical penalties for violation of sections 2511 and 2512, indicating that it viewed possession and sale as negatively as actual interception.[134] Moreover, in *Oceanic*, the court cited a Senate report that indicated that a party "may bring a civil action under § 2520 whether or not the defendant has been subject to a criminal prosecution for the acts complained of."[135]

The majority, on the other hand, asserts that the ECPA did not overrule *Flowers*. The ECPA's legislative history is devoid of any suggestion that Congress intended the revised Act to overrule the *Flowers* precedent. In general, when Congress adopts a new law incorporating sections of an old law, Congress is presumed to be aware of the way in which courts have interpreted the statute.[136] Therefore, the absence of any mention of the *Flowers* decision in the

---

charged with the duty of enforcement of the criminal laws" was narrowly construed to encompass only officers who served on the front line. *Id.* Prosecutors, who did not face the unique risks of serving on the front line, were held not to be among the individuals protected by the law. *Id.*

133. The legislative history of the ECPA suggests that the purpose of the amendment was to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. Specifically, title I of the ECPA expanded the Wiretap Act to "take into account modern advances in electronic telecommunications and computer technology." *Id.* at 3565.

134. 18 U.S.C. § 2511(4)(a) provides that "whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." Section 2512(1) provides that any person who violates this act "shall be fined under this title or imprisoned not more than five years, or both."

135. Oceanic Cablevision, Inc. v. M.D. Elecs., 771 F. Supp. 1019, 1027 (D. Neb. 1991) (citing S. REP. NO. 99-541 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3581).

136. *See, e.g.*, Lorillard v. Pons, 434 U.S. 575 (1978). In *Lorillard*, the Court noted that "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." *Id.* at 580 (citations omitted).

ECPA's legislative history suggests that Congress did not wish to disturb the standing precedent.[137]

Finally, the non-passage of section six of the Motion Picture Anti-Piracy Act[138] cuts in favor of the majority. This bill specifically recommended that section 2520 be amended to provide a civil remedy for any person aggrieved by a violation of section 2512.[139] The fact that Congress considered expanding section 2520 to include certain sections of 2512 but ultimately declined to so provides further evidence that Congress did not intended to supercede *Flowers*. However, most courts give little weight to legislative histories that occur after the enactment of the statute in question.[140]

---

137. *But see* Helvering v. Hallock, 309 U.S. 106 (1940). In *Helvering*, Justice Frankfurter, writing for the Court, indicated that **"**[i]t would require very persuasive circumstances enveloping Congressional silence to debar this Court from reexamining its own doctrines. To explain the cause of non-action by Congress when Congress itself sheds no light is to venture into speculative unrealities." *Id.* at 119–20.

138. S. 1096, 102d Cong., 137 CONG. REC. 11,322 (1991); H.R. 2367, 102d Cong., 137 CONG. REC. 11,240 (1991).

139. S. 1096. The bill's sponsor indicated that its purpose was:

> [To a]mend the Electronic Communications Privacy Act to prohibit devices whose primary purpose or effect is to deactivate copy-protection systems. This provision now carries criminal penalties of up to 5 years imprisonment, a $10,000 fine, or both. The measure would make civil remedies available as well, including injunctions, actual and punitive damages, attorneys' fees and litigation costs.

137 CONG. REC. 11,322.

> Further, section 6 proposed:
>
> (a) Section 2520 of title 18, United States Code (relating to recovery of civil damages) is amended—
>
> (1) by inserting "(1)" before "Except"; and
>
> (2) by adding at the end the following:
>
> "(2) Any person aggrieved by a violation of –
>
> "(A) section 2512(1)(a)(ii),
>
> "(B) section 2512(1)(b)(ii), or
>
> "(C) section 2512(1)(c) to the extent that such section relates to equipment, devices, components, or circuitry described in clause (iii) of such section, may in a civil action recover from any person who engaged in that violation such relief as may be appropriate."

S. 1096.

140. "In evaluating the weight to be attached to [post-enactment statements], we begin with the oft-repeated warning that 'the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one.'" Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.,

C. Policy Rationales

The proponents of the minority position rely heavily on the "private attorney general" argument discussed in *Perez.*[141] The minority argues that allowing private parties to initiate civil suits under section 2520 would not only deter other pirates,[142] but would also "help to guarantee the collapse of the manufacture, distribution, and use network for interception of electronic communications."[143] To support this rationale, minority proponents note that federal prosecutors do not have sufficient time or resources to investigate and litigate these minor, non-violent cases.[144] DirecTV, not the government, suffers the injury; therefore, DirecTV has the incentive to investigate and prosecute.[145]

Further, language of the statute itself indicates not only that Congress intended to allow private rights of action, but also that it wanted to promote such actions. This is evidenced by the fact that the statute grants successful plaintiffs a right to attorney's fees.[146] n

---

447 U.S. 102, 117 (1980) (quoting United States v. Price, 361 U.S. 304, 313 (1960)). *But see* Mont. Wilderness Ass'n. v. U.S. Forest Serv., 655 F.2d 951, 957 (9th Cir. 1981). In *Montana Wilderness Ass'n*, the Ninth Circuit stated that "[a]lthough a subsequent conference report is not entitled to the great weight given subsequent legislation, it is still entitled to significant weight, particularly where it is clear that the conferees had carefully considered the issue." *Id.* (internal citations omitted).

141. DirecTV, Inc. v. Perez, 279 F. Supp. 2d 962 (N.D. Ill. 2003); *see also supra* notes 94–97 and accompanying text.

142. Section 2520 provides for punitive damages in addition to compensatory damages. 18 U.S.C. § 2520(b) (2000). Laws that include punitive remedies are inherently deterrent in nature.

143. *Perez*, 279 F. Supp. 2d at 965. In *Miller v. Webster*, 483 F. Supp. 883 (N.D. Ill. 1979), *rev'd on other grounds sub nom.*, Miller v. Webster, 661 F.2d 623 (7th Cir. 1981), the district court ruled that "the public interest in preventing and discovering illegal wiretaps may be vindicated in some cases only by a private litigant's resort to a civil action under 18 U.S.C. § 2520." *Id.* at 887.

144. *See Miller*, 483 F. Supp. at 890. In *J. I. Case Co. v. Borak*, 377 U.S. 426 (1964), the Supreme Court allowed a stockholder to bring a suit against a public company, even though the statute in question made no explicit mention of a private cause of action. *Id.* at 432. The Court reasoned that "the possibility of civil damages . . . serves as a most effective weapon in the enforcement of [the law]. The [Securities and Exchange] Commission advises that it examines over 2,000 proxy statements annually and each of them must necessarily be expedited. Time does not permit an independent examination of the facts. . . ." *Id.*; *see also* JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 2:1 (2003) (noting that "resources allocated to enforcement of criminal sanctions against illegal surveillance continue to be inadequate").

145. *Perez*, 279 F. Supp. 2d at 965.

146. 18 U.S.C. § 2520 (2000). The statute grants attorneys' fees only to the successful plaintiff, not the prevailing party. *Id.* As such, successful defendants have no statutory right to

addition, section 2520 provides that a successful plaintiff is entitled to the greater of actual damages or statutory damages.[147] An assurance of attorney's fees encourages plaintiffs to initiate litigation.[148]

Section 2520(b) provides for punitive damages.[149] Any statute that provides for punitive damages is designed to have a deterrent effect. When an individual who violates a federal law is punished, the deterrent effect is accomplished regardless of whether the law is enforced by the government or a private party.

Conversely, the majority argues that the statute not only lacks an explicit provision providing a private cause of action, but is also devoid of an implied cause of action.[150] Courts following the majority

---

attorneys' fees. The practical effect of this statute is to mitigate a potential plaintiff's risks; an unsuccessful plaintiff will pay only his or her own attorney's fees, not the defendant's as well. In *Chesny v. Marek*, 720 F.2d 474 (7th Cir. 1983), Judge Posner, writing for the court, ruled that a statute allowing plaintiffs to recover attorneys' fees in civil rights cases was

> intended to encourage the bringing of meritorious civil rights actions . . . "Private attorneys general" should not be deterred from bringing good faith actions to vindicate the fundamental rights . . . by the prospect of having to pay their opponent's counsel fees should they lose. By the same token they should not be deterred from bringing good faith actions to vindicate fundamental rights by the prospect of sacrificing all claims to attorney's fees for legal work at the trial if they win.

Id. at 478–79 (internal citations omitted).

147. 18 U.S.C. § 2520 (2000); *see also* Pac. Harbor Capital, Inc. v. Barnett Bank, N.A., 252 F.3d 1246, 1252 (11th Cir. 2001) (finding that treble damages in a RICO suit encouraged private parties to act as private attorneys general).

148. *See, e.g.*, Buckhannon Bd. & Care Home, Inc. v. W. Va. Dept. of Health & Human Res., 532 U.S. 598, 620 (2001) (holding that a one-sided fee structure indicated that Congress intended to encourage designated private attorneys general to enforce federal law).

149. 18 U.S.C. § 2520(b) (2000).

150. In *Flowers*, the Fourth Circuit noted: "'It is an elemental cannon of statutory construction that where a statute expressly provides a particular remedy or remedies, a court must be chary of reading others into it.'" Flowers v. Tandy Corp., 773 F.2d 585, 589 (4th Cir. 1985) (quoting Transamerica Mortgage Advisers, Inc. v. Lewis, 444 U.S. 11, 19 (1979)). "Congress has expressly provided a criminal sanction against the wiretapper and his agents; we must be wary of reading into the statute a further private civil remedy against the seller of a device primarily useful for wiretapping." *Flowers*, 773 F.2d at 589.

In one of its most recent pronouncements on implied rights of action, the Supreme Court noted:

> Like substantive federal law itself, private rights of action to enforce federal law must be created by Congress. The judicial task is to interpret the statute Congress has passed to determine whether it displays intent to create not just a private right but also a private remedy. Statutory intent on this latter point is determinative. Without it, a

approach, including the Fourth Circuit, have ruled that Congress enacted section 2512, a criminal statute, to protect the public as a whole.[151] As such, these courts have declined to hold that conduct prohibited in section 2512 can serve as the basis for a civil action under section 2520.

Article III of the United States Constitution requires that a plaintiff prove that he or she suffered actual harm as a result of the defendant's conduct to have proper standing for federal jurisdiction.[152] The Supreme Court has interpreted this to mean that the injury must be "distinct and palpable," and not "abstract," "conjectural," or "hypothetical."[153] The majority courts have held that proof of mere possession of a pirate access device proves nothing more than a hypothetical harm.[154]

Federal courts, including the Supreme Court, have commented that, whenever possible, statutes should be interpreted narrowly to avoid constitutional infirmities.[155] As applied to section 2520, this

---

> cause of action does not exist and courts may not create one, no matter how desirable that might be as a policy matter, or how compatible with the statute.

Alexander v. Sandoval, 532 U.S. 275, 286–87 (2001) (internal citations omitted).

151. *Flowers*, 773 F.2d at 589. In *Cort v. Ash*, 422 U.S. 66 (1975), the Supreme Court articulated four factors that a court should consider in determining whether a statute provides a private right of action:

> First, is the plaintiff "one of the class for whose *especial* benefit the statute was enacted" . . . that is, does the statute create a federal right in favor of the plaintiff? Second, is there any indication of legislative intent, explicit or implicit, either to create such a remedy or to deny one? Third, is it consistent with the underlying purposes of the legislative scheme to imply such a remedy for the plaintiff? And finally, is the cause of action one traditionally relegated to state law, in an area basically the concern of the States, so that it would be inappropriate to infer a cause of action based solely on federal law?

Id. at 78 (internal citations omitted). Since *Cort* was decided in 1975, this test has declined in popularity. Courts are more likely to use the intent test articulated in *Alexander*. *See supra* note 150.

152. U.S. CONST. art III; *see also* Lujan. v. Defenders of Wildlife, 504 U.S. 555, 560 (1992); *supra* note 119 and accompanying text.

153. Allen v. Wright, 468 U.S. 737, 751 (1984) (internal citations omitted).

154. *See, e.g.*, DirecTV, Inc. v. Treworgy, 373 F.3d 1124, 1127 (11th Cir. 2004).

155. *See* NLRB v. Catholic Bishop, 440 U.S. 490 (1979). In *Catholic Bishop*, Catholic schools refused to bargain with local labor unions. *Id.* at 495. The unions filed an unfair labor practice suit with the National Labor Relations Board (NLRB). *Id.* The schools argued that the NLRB did not have jurisdiction over them on both statutory and constitutional grounds. *Id.* The

presumption cuts in favor of the majority. Without clear intent to the contrary, a court should construe the statute to allow only private parties who have suffered *actual* harm, and who thus have a case or controversy as defined by the Constitution, to bring suit under section 2520 in federal court.

Support for this argument can be found in the plain language of section 2520. Specifically, the statute indicates that a plaintiff "may in a civil action *recover* from the person or entity which engaged in that violation such *relief* as may be appropriate."[156] The words "recover" and "relief" both indicate Congress' intent to create a compensatory provision. By definition, compensatory, or actual, damages are designed to make a plaintiff who suffered a specific injury as a result of the defendant's conduct whole.[157] When there is no proof of actual harm, compensatory remedies, such as those provided in section 2520(a), are inapplicable.

A related consequence of the minority's interpretation is the possibility that alleged pirates could be liable to multiple plaintiffs. If a plaintiff need not procure proof of actual harm to file suit under sections 2512 and 2520, any party whose signals hypothetically *could* have been intercepted would have standing. It is unlikely that Congress intended to put unlimited liability on undeserving parties.

Finally, given the various applications of the equipment used by pirates to intercept DBS signals, innocent parties could be wrongly prosecuted. William Blackstone famously wrote that "the law holds, that it is better that ten guilty persons escape, than one innocent person suffer."[158] Accordingly, liberty and equity mitigate towards the majority's position.[159]

Court construed the statute in favor of the schools to avoid issues concerning the Establishment Clause of the First Amendment. *Id.* at 508.

156. 18 U.S.C. § 2520(a) (2000) (emphasis added).

157. BLACK'S LAW DICTIONARY 416 (8th ed. 2004). Black's defines compensatory damages, or actual damages, as "[a]n amount awarded to a complainant to compensate for a proven injury or loss; damages that repay actual losses." *Id.*

158. 4 WILLIAM BLACKSTONE, COMMENTARIES 352 (1769).

159. The rule of lenity provides a related consideration. The rule suggests that "a court, in construing an ambiguous criminal statute that sets out multiple or inconsistent punishments, should resolve the ambiguity in favor of the more lenient punishment." BLACK'S LAW DICTIONARY 1359 (8th ed. 2004). The question is whether the statute at issue made it reasonably clear at the time that the alleged misconduct occurred that the conduct was illegal. United States v. Lanier, 520 U.S. 259, 265–66 (1997). If the section lacks clarity, the rule

IV. CONCLUSION

The proponents of the minority position advance an intuitively pleasing argument. When a consumer purchases a pirate access device, it would not be unreasonable for a court to recognize a rebuttable presumption that the consumer used the device for its intended purpose and injured the DBS provider. Moreover, in the absence of any legislative history to the contrary, it seems that the only reason Congress passed the ECPA was to provide a private cause of action against any violation of the Wiretap Act. In sum, the minority believes that DirecTV should be able to protect its intangible property from unscrupulous pirates.

However, the federal courts have made it clear that statutory interpretation begins with the language of the statute. Though the words of the Wiretap Act do not project a crystal clear meaning, the scales tip in favor of the majority's interpretation. Moreover, a narrow interpretation minimizes the potential for constitutional infirmities and wrongful convictions.

---

indicates that the statute should be interpreted as narrowly as reasonably possible. *Id.* at 266. In part, the rationale behind this rule is that due process requires "fair warning . . . of what the law intends." *Id.*; *see also* McBoyle v. United States, 283 U.S. 25, 27 (1931). Though generally discussed in criminal cases, the rule of lenity has been applied in other contexts as well. In *United States v. Thompson/Center Arms Co.*, 504 U.S. 505 (1992), the Court applied the rule of lenity to a tax statute in a civil case. *Id.* at 517–18. In the instant case, the split of authority was patent evidence that the statute lacked clarity. As such, under the rule of lenity, the statute should be narrowly construed to exclude incorporation of the criminal statute, section 2512.