THE UNUSUAL SUSPECTS: UNSCRAMBLING SATELLITE PIRACY

DAVID V. LAMPMAN, II*

TABLE OF CONTENTS

* J.D. Albany Law School, Union University, May 2003; B.A. King's College 2000. Editor-in-Chief, *Albany Law Journal of Science & Technology*, 2002–2003. Special thanks to Professor Moriarty for his numerous suggestions concerning an earlier draft of this Article. I would like to thank Wayne A. Smith Jr., Esq. for his interest and editorial comments related to this Article. Additionally, I would like to express thanks to my family for their continued encouragement and love.

INTRODUCTION

> I thought we were going to get television. The truth is television is [going to] get us.[1]

> They may not wear eye patches or wield swords whilst shouting (Avast Mateys) as their forerunners of centuries ago did, but there are some new swashbuckling pirates across North America whose haul is far greater than any legendary ship's bounty. These buccaneers wear three-piece business suits, or loll about in tatty T-shirts and mangy sweatpants in front of home computers as they devote their time and energy to stealing something considered to be far more valuable than gold doubloons—satellite television signals.[2]

Technological developments spur change and become the catalysts for revolution.[3] Of course, while particular technologies have changed, this has been the case for some time.[4] In fact, the principal revolutions that were central to the development of Western Civilization were the product of technology.[5] Currently, communication, computer, and digital technologies are driving the development of the Information Age.[6] However, as technology

---

1 QUIZ SHOW (Hollywood Pictures 1994) (quoting Richard Goodwin).

2 John Pifer, *Signal Snatchers: Subterfuge, Espionage, and Genius . . . The Multi-Billion-Dollar Theft of TV Satellite Signals*, BC BUS. MAG. (Feb. 2003), *at* http://www.bcbusinessmagazine.com/displayArticle.php?archive=ARC&artId=265 (last visited Aug. 8, 2004).

3 *See* Colin B. Picker, *A View From 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOZO L. REV. 149, 151 (2001); *see also* Brian Paul Menard, *E-Commerce in the Digital Millennium: The Legal Ramifications of the DMCA and Business Method Patents: And the Shirt Off Your Back: Universal City Studios, DECSS, and the Digital Millennium Copyright Act*, 27 RUTGERS COMPUTER & TECH. L.J. 371, 373 (2001); *see generally, A Brief History of Technology*, COMM. & THE ARTS, *available at* http://www.regent.edu/acad/schcom/rojc/mdic/history.html (last visited Aug. 8, 2004); Peter F. Drucker, *The First Technological Revolution And Its Lessons* (discussing the first industrial revolution), *at* http://xroads.virginia.edu/~DRBR/d_rucker5.html (last visited Aug. 8, 2004).

4 *See* Picker, *supra* note 3, at 151.

5 *See* Blake L. White, *The Structure of Paradigm Change in Science and Technology*, STRATEGIC TECH. INST., *at* http://www.strategic-tech.org/images/structure_of_Scientific_and_Technological_change.pdf (last visited Feb. 8, 2004).

6 *See* President Bill Clinton, Remarks by The President at Massachusetts Institute of Technology 1998 Commencement (June 5, 1998), *available at* http://clinton2.nara.gov/WH/New/html/19980605-28045.html (last visited Feb. 25, 2003) [hereinafter Remarks].

forces rapid change, social institutions and the law often struggle to keep pace.[7] Unfortunately, the Information Age has not been able to escape this trend.[8] Consequently, it is causing confusion and change in constitutional law,[9] criminal law,[10] and intellectual property law.[11]

This Article will address satellite technology, a vital component in the progress of the Information Age. Specifically, it will examine the issue of satellite piracy and will focus on the theft of digital television signals. The scope of this Article will concentrate on a white collar crime analysis of satellite television piracy, which is accomplished by using illegal circumvention techniques.[12] Since 1977, the Department of Justice ("DoJ") has included illegal circumvention in its definition of white collar crime.[13]

Part I of this Article will provide a background of the satellite industry.[14] This Part will lay the foundation of this Article by explaining the importance of satellite technology and in particular, satellite television. Part II will assess the practice of pirating satellite television.[15] This Part will operate under the assumption that knowledge of how satellite pirates perform will aid law enforcement in prosecuting this crime. It will also discuss piracy's negative impact on technological and economic development.

Part III will identify and evaluate the laws that criminalize satellite piracy and the liability of each class of pirate.[16] This Part will attempt to illustrate that the use of general laws and considerations that often aid in the prosecution of other white collar criminals will be potent additions in stopping this crime. Specifically, it will dis-

---

[7] *See* Picker, *supra* note 3, at 151; Alan Heinrich, et al., *At The Crossroads of Law and Technology*, 33 LOY. L.A. L. REV. 1035, 1042 (2000); *see also* CRAIG JOYCE ET AL., COPYRIGHT LAW 49 (5th ed. 2001).

[8] *See* Heinrich, *supra* note 7, at 1036. Heinrich predicts that:

> The information revolution underway will change law as nothing in our experience or understanding has. It took a millennium to develop a sophisticated common law regime, one based on rights, property, and regulation. It may take less than a decade for that regime to unravel, as core concepts lose meaning. Not surprisingly, we are unprepared.

Id.; *see also* Remarks, *supra* note 6 (addressing the challenges of the Information Age).

[9] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (addressing the issues of police technologies and privacy rights under the Fourth Amendment).

[10] *See id. See generally* A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW (2001).

[11] *See* SCOTT, *supra* note 10, at 6–7.

[12] JULIE R. O'SULLIVAN, FEDERAL WHITE COLLAR CRIMES 5 (2001).

[13] *See id.* "White-collar offenses shall constitute those classes of non-violent illegal activities which principally involve traditional notions of deceit, subterfuge or *illegal circumvention.*" *Id.* (quoting U.S. DEP'T OF JUSTICE NATIONAL PRIORITIES FOR WHITE-COLLAR CRIME 5 (1977) (emphasis added)).

[14] *See infra* notes 19–109 and accompanying text.

[15] *See infra* notes 110–212 and accompanying text.

[16] *See infra* notes 213–450 and accompanying text.

cuss the mail and wire fraud acts and their application to intellectual property crimes. Part IV will conclude this Article by addressing the need for legislation that is specific to the crime of satellite piracy.[17] It will also provide suggestions that may help to arrest, prosecute, and deter individuals interested in committing this crime.[18] In doing so, this Article will advocate for American society, and specifically for Congress, to strike a balance between consumers and information providers. In brief, it will argue that consumers must not pirate intellectual property, and that providers cannot overprotect their intellectual property. Therefore, there must be a mutual respect for the expression of ideas and for the access to those ideas — the Information Age will only thrive in such an environment.

I. THE SIGNIFICANCE OF SATELLITE TECHNOLOGY

A. *The Rise of the Satellites*

1. The Soviets Strike First

In October of 1945, the author of 2001: A SPACE ODYSSEY, Arthur C. Clarke, theorized in a technical essay that if an artificial satellite was positioned high enough above the equator, it would be able to equal the earth's orbit.[19] Clarke believed that the satellite would appear to be set in the sky, which would allow it to send radio and television signals around the world.[20] At the time, Clarke's vision seemed to be as far-fetched and as perplexing as his great novel; nevertheless, technology eventually substantiated his hypothesis.[21] In fact, it only took scientists a dozen years to the month to lay the keystone support that would make Clarke's improbable piece of science fiction become science fact.[22]

The first artificial satellite to orbit the earth was only the size of a basketball, simply capable of transmitting a series of beeps, and only survived for ninety-two days.[23] However, at the time, it was symbolic of twentieth century technological progress, a na-

---

17 *See infra* notes 451–457 and accompanying text.

18 *See* O'SULLIVAN, *supra* note 12, at 5.

19 *See* PACIFIC SATELLITE, *Satellite History*, *at* http://www.pacificsatellite.com/project2.php (last visited Aug. 30, 2004).

20 *See id.*

21 *See id.*

22 *See generally id.*

23 *See* NASA, *Sputnik and the Dawn of the Space Age*, *at* http://www.hq.nasa.gov/office/pao/History/sputnik/index.html (last visited Aug. 30, 2004) [hereinafter *Sputnik and the Dawn of the Space Age*]; *see also* NAUTS, *Sputnik Satellites and Launch Vehicles* (noting that Sputnik only returned signals for twenty-one days), *at* http://www.nauts.com/vehicles/50s/sputnik.html (last visited Mar. 10, 2003) [hereinafter *Sputnik Satellites and Launch Vehicles*].

tion's failure to keep pace with that progress,[24] and the commencement of the space race.[25] Of course, this infamous satellite was the USSR's Sputnik I that was launched on October 4, 1957.[26] Again, on November 3, 1957, the Soviets bested the United States by launching Sputnik II,[27] which marked the first time a living organism, a dog named Laika, entered outer space.[28] Sputnik II was a heavier satellite than Sputnik I; more importantly, Sputnik II transmitted the complex data of Laika's biological information.[29] Not only was this an important moment in the evolution of satellite technology, it was also a step forward in the race to send a human to outer space.[30] Acknowledging the progress of the Soviets, the United States government knew that it had to respond to the success of Sputnik with its own technological opus in order to participate in space discovery and perhaps, more importantly, to reassure the American people of the nation's clout.

2. The United States Takes the Lead

Finally, on January 31, 1958, the United States struck back by

---

[24] *See* Henry Wong, Comment, *2001: A Space Legislation Odyssey - A Proposed Model For Reforming The Intergovernmental Satellite Organizations*, 48 AM. U. L. REV. 547, 551 (1998) (noting that "[m]any Americans believed that the 'race to space' would determine the outcome of the Cold War"). Therefore, the USSR's success with Sputnik worried Americans who, prior to October 4, 1957, believed that the USA was a technologically superior nation. *See id.*; *Sputnik and the Dawn of the Space Age*, *supra* note 23 ("Sputnik caught the world's attention and the American public off-guard . . . the public feared that the Soviets' ability to launch satellites also translated into the capability to launch ballistic missiles that could carry nuclear weapons from Europe to the U.S."); PAUL DICKSON, SPUTNIK: THE SHOCK OF THE CENTURY—*Sputnik Memories and Comments*, *at* http://www.sputnikbook.com/comments.php (last visited Aug. 10, 2004). The author records Chris Kuppig's recollection of the USSR's launching of Sputnik:

> I was nine at the time, growing up within 25 miles of Strategic Air Command headquarters, and just a few years beyond my literal understandings of such things as the 'Iron Curtain'—which I previously believed to be some kind of chain-mail drapery that I actually might be caught behind. Suddenly, there was a new Communist threat passing right overhead, and I recall spending many a dinnertime trying to convince my parents of our need for a bomb shelter.

Id.; *see also* DAVID E. LUPTON, ON SPACE WARFARE: A SPACE POWER DOCTRINE 70 (1998), *available at* http://www.maxwell.af.mil/au/aul/aupress/Books/Lupton/lupton.pdf (last visited Aug. 30, 2004).

[25] *See* John J. Gibbons, *Convergence in Communications Technology and The First Amendment*, 25 SETON HALL L. REV. 1375, 1390 (1995) (stating that Sputnik was directly responsible for the conception of NASA); The National Aeronautics and Space Act of 1958, Pub. L. No. 85-568, 72 Stat. 426, 42 U.S.C.A. 2451 (1995); *see Sputnik and the Dawn of the Space Age*, *supra* note 23; LUPTON, *supra* note 24, at 70.

[26] *See, e.g.*, *Sputnik and the Dawn of the Space Age*, *supra* note 23.

[27] *See Sputnik Satellites and Launch Vehicles*, *supra* note 23; Alan Ladwig, *Explorer I – The 42nd Anniversary of America's First Satellite*, SPACE.COM, Jan. 31, 2000 (stating that Sputnik II weighed 1,200 pounds, almost 1,000 pounds more than Sputnik I), *at* http://www.space.com/news/explorer_anniversary_000127.html (last visited Aug. 30, 2004).

[28] *See id.*

[29] *See id.*

[30] *See id.* (noting that the information showed that Laika was adjusting to space).

launching the Explorer I satellite, which marked the beginning of a shift of power and success in the space race.[31] The Explorer I launch was the first of four successful Explorer missions that took place between 1958 and 1959.[32] However, the Explorer satellite launches were only the beginning of America's space and satellite experimentations; in fact, the United States space program was advancing at a very rapid pace.[33] This was evident in August of 1960, when the National Aeronautics and Space Administration ("NASA") launched the Echo I satellite, which was the first passive communications satellite.[34] Because Echo I was a passive satellite, it was only capable of reflecting radio signals.[35] Thus, it could not "actively receive, amplify, or transit" signals.[36] NASA solved this shortcoming by launching Telstar I, which was the first satellite that was able to amplify the signals it received, and send those signals back to various ground stations.[37] "Telstar [I] successfully relayed the first transatlantic television signals and inaugurated a new age in communications."[38]

Furthermore, Telstar I was the first satellite project supported by a nongovernmental organization; it was a joint venture between American Telephone and Telegraph Company ("AT&T") and NASA.[39] Indeed, it was AT&T's John R. Pierce who was the first to fully evaluate the technological options in satellite communications and to recognize the financial potential in satellite communications.[40] When Congress realized that private corporations had

---

31 *See* Ernst Stuhlinger, *Reminiscences of Explorer 1*, ASTRODIGITAL, *at* http://www.astrodigital.org/space/explorer1.html (Wernher Von Braun, the great pioneer of space exploration stated: "We have now established our foothold in space, we will never give it up again.") (last visited Aug. 30, 2004); *Sputnik and the Dawn of the Space Age*, *supra* note 23 (noting that this "satellite carried a small scientific payload that eventually discovered the magnetic radiation belts around the Earth" and aided in the development of spacecraft); REDSTONE ARSENAL, *The Story of the Army's Satellite Program* (stating that the United States Army was instrumental in the success of early satellites and that Explorer I collected a great deal of valuable data concerning outer space), *at* http://www.redstone.army.mil/history/explorer/explorer.html (last visited Aug. 30, 2004) [hereinafter REDSTONE ARSENAL]; Ladwig, *supra* note 27 (noting that Explorer I only weighed eighteen pounds).

32 *See* NAT'L ACADEMIES, *The National Academy of the Sciences and the First U.S. Satellite*, *at* http://www.nas.edu/history/explorer/ (last visited Aug. 30, 2004).

33 *See id.*

34 *See Dwight D. Eisenhower, 34th U.S. President Gives First Speech Bounced Off A Satellite*, HISTORY CHANNEL.COM, *at* http:// www.historychannel.com/speeches/archive/speech_440.html (last visited Aug. 30, 2004).

35 *See id.*

36 *Id.* (noting that Echo I was the largest satellite ever launched).

37 *See id.*

38 *Id.*

39 *See* David J. Whalen, *Communications Satellites: Making the Global Village Possible*, NASA, http://www.hq.nasa.gov/office/pao/History/satcomhistory.html (last visited Aug. 30, 2004).

40 *See id.* (noting that Pierce, now a billionaire, first made his claims in a 1954 speech).

an interest in the development of satellites, it passed the Communications Satellite Act of 1962 ("CSA"),[41] which was designed to create a global communication system.[42] The CSA, in order to achieve its goal, "authorized the Congressionally-chartered, private corporation, the Communications Satellite Corporation ("Comsat")."[43] Comsat was dominated by private industry; however, it was regulated and supported by the FCC.[44] In essence, it was "a quasi-private, quasi-governmental entity" that had the task of accomplishing the full potential of satellite technology.[45] When Comsat was established, it would have been difficult, perhaps impossible, to fathom the impact and success it would have on global communications.[46]

> When Apollo 11 landed on the moon in 1969, the images of the event were carried live via satellite to millions of people worldwide. As a result of a global commercial satellite system, it was the most widely viewed event in broadcast history. As astronaut Neil Armstrong announced that he had taken 'one small step for man, one giant leap for mankind,' Americans at last were able to shed their insecurity over Sputnik. Congress' repeated attempts to ease the national conscience had finally manifested itself through the legacy of the C[ommunications] S[atellite] Act. From that point forward, America would regain the lead in the space race. More importantly, however, these satellite images marked the beginning of a period that would change forever conventional views of the universe and the world's relationship to the cosmos.[47]

Therefore, what began as a game to keep up with the Soviets turned into a game of exploration and technological innovation, the fruits of which are still evident and are, indeed, still unfolding. It is, of course, ironic that the genesis of satellite technology, which was at first an earth-shaking success for the communist Soviets and

---

41 47 U.S.C. 701 § 102 (2000); *see* Whalen, *supra* note 39; Wong, *supra* note 24, at 551 (noting that "the CS Act represented the first international attempt at commercial space activity").

42 *See* Henry Goldberg, *50th Anniversary of the Communications Act: Special Supplement: One-Hundred And Twenty Years of International Communications*, 37 FED. COMM. L.J. 131, 141 (1985) (providing that the United States had companies that possessed the manufacturing means to lead the satellite revolution).

43 *Id.* "Comsat had among its directors three individuals appointed by the President and confirmed by the Senate. Fifty percent of the stock was to be owned by the international carriers, including AT&T, and the balance was to be made available in what was to be a wildly successful public offering." *Id.*

44 *See id.* at 142.

45 *Id.*

46 *See* Wong, *supra* note 24, at 552.

47 *Id.*

a crushing failure for the capitalist Americans, has now blossomed into an entrepreneurial venture that is a multi-billion dollar industry and one of the catalysts of the Information Age.[48] It is equally ironic that the merger of these competing ideologies now threatens satellite technology, specifically satellite television. As will be illustrated in Part II of this Article, satellite television piracy is driven by two basic motives: (1) the "communistic" ideals of the encryption hackers who believe that satellite signals should not be protected as property rights; and (2) the profit seeking individuals who market the hackers information.[49]

B. *Contemporary Satellite Industry: Technological & Economic Consequence*

1. The Technological Consequence

Today, satellite technologies serve to support both technological and economic development.[50] Unmistakably, satellites are improving telephone, television, radio, and Internet broadcasts, thereby acting as the foundation for the Information Age.[51] However, their utility extends far beyond these popular uses.[52] In fact, satellites seem to play a role in every aspect of life, extending the Information Age beyond fast information, perfect digital copies, and high quality resolution.

---

48 *See infra* notes 65–72 and accompanying text.

49 CYBERCRIME: LAW ENFORCEMENT, SECURITY AND SURVEILLANCE IN THE INFORMATION AGE 6–7 (Douglas Thomas & Brian D. Loader eds., 2000) (noting that pirate hackers are not motivated by financial gain) [hereinafter CYBERCRIME]; CHARLES PLATT, ANARCHY ONLINE 11, 103 (1997) (stating that hackers have a disdain for capitalistic ideology of maximizing profit and an underlying distrust for the government).

50 *See* Joe Pelton, *Satellites Can Rise Above Disaster*, SATELLITE NEWS, Feb. 10, 2003; Cyrus D. Jilla & David W. Miller, *Satellite Design: Past, Present and Future* (1997) (unpublished manuscript) (on file with the Department of Aeronautics and Astronautics, Massachusetts Institute of Technology), http://www.ee.surrey.ac.uk/SSC/CSER/UOSAT/IJSSE/issue1/cjilla/cjilla.html (last visited Aug. 30, 2004).

51 *See* PIPPA NORRIS, DIGITAL DIVIDE? 5, 12, *available at* http://ksghome.harvard.edu/~.pnorris.shorenstein.ksg/acrobat/digitalch1.pdf (last visited Aug. 30, 2004).

52 *See* Pelton, *supra* note 50. For example:

> Without global positioning and space navigation satellites, scores of important tasks that we now take for granted would be extremely difficult or even impossible. Those global positioning and navigation satellites aid with the take off and landing of aircraft, the steering of ships, tankers and aircraft carriers, the location of downed aircraft, the routing of trains and the operation of 911 rescue activities around the world. . . . Satellites . . . [have] saved perhaps hundreds of thousands of lives. These space systems have saved entire towns and cities by warning of hurricanes, monsoons, tropical storms and tornadoes. We now understand the global impact of El Nino and La Nina and other global weather conditions. Farmers and fisherman [sic] likewise have avoided many billions of dollars in losses . . . Most recently, we have found the need to use satellites to protect against terrorist attack, the poisoning of water supply and the development of weapons of mass destruction.

Id.

Indeed, satellites are used as tools by various governmental agencies, commercial industries, and individuals.[53] Fittingly, since the military played an important role in their germination,[54] satellites are frequently and efficiently used in military surveillance and strikes.[55] Also, they are used to monitor the security of homes and the health of individuals.[56] Furthermore, they track automobiles,[57] children,[58] criminals[59] endangered species,[60] and even the supply and location of food in developing countries.[61] Additionally, they can forecast the weather and predict and track the outbreak of diseases.[62] They are also a valuable mapping and survey tool.[63] For example, they are used as an economical way to estimate the damage of a natural disaster.[64]

2. The Economic Consequence

In 1997, American companies controlled forty-five percent of the commercial satellite industry's global revenues, which exceeded fifty-one billion dollars.[65] More than a third of these reve-

---

53 *See generally* Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 987 (1983) ("Satellites circling the globe can place an electronic eye over a third of the earth's surface, collect information, and deliver it to any other spot on earth instantaneously.").

54 *See* Ladwig, *supra* note 27; REDSTONE ARSENAL, *supra* note 31.

55 *See, e.g.*, Douglas A. Macgregor, *Resurrecting Transformation: A New Structure for Post-Industrial Warfare*, DEF. HORIZONS, Sept. 2001, at 3, 7, *available at* http://www.comw.org/qdr/fulltext/0109macgregor.pdf (last visited Aug. 30, 2004); *see* Tom Infield, *U.S. Has Refined Its Weapons, Vastly Improved Surveillance*, SEATTLE TIMES, Oct. 6, 2001, at A4; Clayton Mowry, *Satellites Save Lives*, SATELLITE COMM., Feb. 1999, at 70 (reporting various uses of satellites to track lost individuals and to transmit life saving information).

56 *See Wireless Home Security and Alarm System*, SAFETY & SECURITY CTR. (featuring a GPS home security system and a GPS Watch for Alzheimer's patients), *at* http://www.wirelesshomesecurityalarmsystems.com (last visited Mar. 11, 2003).

57 *See, e.g.*, David Hayes, *Global Positioning Gear Propels Olathe, Kan.-Based Tech Company's Growth*, KAN. CITY STAR, Feb. 13, 2003, at A1.

58 *See* Jane Spencer, *Tracking the Kids by Satellite*, WALL ST. J., Feb. 18, 2003, at D1.

59 *See Local Agencies Use GPS to Track Convicts, Vehicles*, SATELLITE NEWS, Sept. 9, 2002.

60 *See, e.g.*, *Rare Sea Turtle Returns to Wild After Treatment*, SEATTLE TIMES, Oct. 16, 2000, at B3.

61 *See* C.K. Prahalad & Allen Hammond, *Serving the World's Poor, Profitably*, HARV. BUS. REV., Sept. 2002 (reporting that satellite tracking systems are able to locate schools of fish), at 6, *available at* http://www.cme-mec.ca/shared/upload/paper.pdf (last visited Mar. 11, 2003).

62 *See, e.g.*, David E. Steitz, *Satellites Used To Help Predict Disease Outbreaks*, NASA, July 15, 1999, *available at* http://web.ask.com/redir?bpg=http%3a%2f%2fweb.ask.com%2fweb%3fq%3dwhat%2bare%2bsatellites%2bused%2bfor%26o%3d0&q=what+are§atellitesšedôr&u=http%3a%2f%2fwww.earth.nasa.gov%2febn%2fnews00016.html&s= (last visited Mar. 11, 2003).

63 *See* PARTNER RES., *The Use of Satellites for Flood Loss Estimation*, Oct. 2001, at 1, *available at* http://216.239.51.100/search?q=cache:R-U2MNaJCIkC:www.partnerre.com/pdf/Flood-Satellite.pdf™heše+of§atellites+&hl=EN&ie=UTF-8 (last visited Mar. 10, 2003).

64 *See id.*

65 *See U.S. Dominates $50 Billion Global Satellite Industry, Sia Says*, SATELLITE NEWS, Apr. 20, 1998 [hereinafter *Global Satellite Industry*].

nues were generated by satellite services.[66] Between 1996 and 1997, the value of the industry grew by more than fourteen percent.[67] In 2001, when both growth and revenue were plummeting in other sectors, the satellite industry was worth more than eighty-five billion dollars.[68] More impressively, it had a growth rate of eighteen percent.[69] From 1996 to 2002, the satellite services industry tripled in size.[70] The rapid and sustaining growth in this area of the industry is attributed to the boom in satellite television.[71] Furthermore, on a global scale the industry employs nearly 200,000 people, and sixty-one percent of these jobs are in the United States.[72]

Still, satellites serve a more fundamental purpose in today's economy than generating profit.[73] Satellite communications have the potential to increase the availability of goods and services in less developed regions and to stoke investment in these areas.[74] Moreover, they will enable these commodities to be delivered to end users at a low cost.[75] They are key to the access of global information networks.[76] More importantly, they are an efficient means for the developing nations to achieve this access and to participate in the Information Age.[77] There should be no doubt that if the Information Age is to reach its full potential of globalization and the efficient diffusion of knowledge, industries that create and support satellite technology must be constantly supported with investment. Correspondingly, it is important that the satellite industry is a safe investment.[78]

---

66 *See id.*

67 *See id.*

68 *See* Paul Dykewicz, *Satellite Recovery Stalled By Telecom*, SATELLITE NEWS, Aug. 5, 2002.

69 *See id.*

70 *See id.*

71 *See, e.g., id.*

72 *See Global Satellite Industry*, *supra* note 65.

73 *See, e.g.*, Frank Morring Jr. & Michael A. Taverna, *Satellites Seen as Bridge over 'Digital Divide,'* AVIATION WK. & SPACE TECH., Oct. 29, 2001, at 86; *see also* Whalen, *supra* note 39 ("Satellite communications is also the only truly commercial space technology generating billions of dollars annually in sales of products and services.").

74 *See* Lee Berger, Comment, *Proposed Legal Structure For The Silksat Satellite Consortium: A Regional Intergovernmental Organization to Improve Telecommunications Infrastructure in Central Asia and the Trans-Caucasus Region*, 33 LAW & POL'Y INT'L BUS. 99, 104 (2001).

75 *See id.*

76 *See* Morring & Taverna, *supra* note 73, at 86.

77 *See id.*

78 *See supra* note 71 and accompanying text (noting that the satellite television is the most economically successful wing of the satellite industry). Satellite television is also responsible for developing new technology that will serve to promote the development of the Information Age.

C. *Satellite Television*

1. The Development of Satellite Television

Although the achievement of sending the first television signals to earth via satellite was accomplished in the 1960s, the widespread use of satellites for television viewing is only twenty-nine years old.[79] In 1975, Home Box Office ("HBO") used RCA's Satcom I satellite[80] to deliver its subscription television service to its local cable affiliates.[81] The local cable affiliates would then deliver it to HBO's viewers.[82] It is important to note that HBO's decision to use satellites was a matter of necessity.[83]

HBO began to offer its subscription services in 1972 by sending its signals through a network of microwave towers.[84] In this system, each tower was linked so that the signal could be relayed from point to point.[85] Obviously, this was very expensive; it was also inefficient and difficult to maintain.[86] While there was a heavy demand for HBO's programming, the networking system limited their ability to reach consumers.[87] This dilemma threatened HBO and cable television, in general.[88] In fact, in 1973, HBO only had 8000 customers and was "struggling to survive."[89] However, by 1977, less than two years after HBO began to use Satcom I, it had more than 1.6 million subscribers.[90] In brief, satellites changed the distribution and the form of television and set the stage for further developments in the Information Age.

2. The Advantages Associated with Satellite Television

Satellites offer advantages to television viewing beyond the issue of distribution. The advantage most commonly recognized is that satellite television offers higher quality digital picture and

---

79 *See* ASS'N, *Satellite Television Industry Celebrates Its 25th Anniversary*, SATELLITE BROADCASTING & COMM., *at* http://www.sbca.com/press/Aug02b-01.htm (last visited Aug. 30, 2004).

80 *See* Kevin S. Forsyth, *Delta, Satcom, and the Cable Boom* (noting that Satcom I was developed by RCA, McDonnell Douglas, and NASA and was launched on December 13, 1975), *at* http://kevin.forsyth.net/delta/satcom.htm (last visited Aug. 30, 2004).

81 *See* Michael Piscitelli, *Home Satellite Viewing: A Free Ticket to the Movies?*, 35 FED. COMM. L.J. 1, 1 (1983) (analyzing the legal issues involved in the interception of satellite television signals); Steven DeBaun, Comment, *The Piracy of Subscription TV — A Market Place Solution to the Unauthorized Interception of MDS Transmissions*, 34 UCLA L. REV. 445, 445 (1986).

82 *See* DeBaun, *supra* note 81, at 445.

83 *See* Forsyth, *supra* note 80.

84 *See id.*

85 *See id.*

86 *See id.*

87 *See id.*

88 *See id.*

89 *See* Forsyth, *supra* note 80.

90 *See id.*

sound than analogue distribution or receiving services.[91] It also improves distribution of pay television by allowing individuals living in rural areas not serviced by cable outlets to access premium television.[92] Furthermore, it introduces the concept of "free will" to television; it offers more channels and more options in direct purchase viewing.[93] For example, many satellite television companies contract with professional sports leagues to broadcast every game that the league schedules in a season, and then offers "season tickets" to television viewers.[94] This is important to viewers who follow a team that is not covered by their local networks.[95] Similarly, satellite television allows viewers to access broadcasts from foreign nations.[96]

3. The Economic Worth of Satellite Television

As previously noted, satellite television is the fastest growing sector of the satellite industry.[97] It is driving the growth and development of the satellite industry and the technologies that support it.[98] It is also one of the fastest selling consumer electronic products marketed in the United States.[99] In fact, in its first ten years it grew faster than color television, cable television, VCRs, and CDs.[100] "In just over seven years, [1995-2002] direct broadcast satellite ('DBS') has grown to over 16.7 million households—representing over forty-four million viewers."[101] In 2002, the market in the United States was worth twelve billion dollars, and the Canadian market was worth an additional $1.26 billion.[102] It is projected that by 2008, satellite television will be in thirty-four million homes and will be worth $24.3 billion in North America alone.[103]

Further, satellite television benefits the economy in other

---

91 *See* James Sterngold, *Murdoch and Echostar to Create Big Satellite TV Operation*, N.Y. TIMES, Feb. 25, 1997, at D1.

92 *See* Geraldine Fabrikant & Seth Schiesel, *Satellite v. Cable: A Rivalry Beyond TV*, N.Y. TIMES, Feb. 19, 2001, at C1.

93 *See id.*; *see also* Sterngold, *supra* note 91, at D1.

94 Fabrikant & Schiesel, *supra* note 92, at C1.

95 *See id.*

96 *See id.*

97 *See supra* note 71 and accompanying text.

98 *See supra* note 71 and accompanying text.

99 *See* Jimmy Schaeffler, *DBS is Growing at a 'Remarkable Pace'*, SATELLITE NEWS, July 29, 2002; *see also* Andy Wright, *Satellite Television Continues to be a Value Leader*, TWICE, Jan. 8, 2002, *available at* http://www.twice.com/index.asp?layout=story_stocks&articleid=CA190124 (last visited Mar.15, 2003).

100 *See* Schaeffler, *supra* note 99.

101 Wright, *supra* note 99 (reporting that when C band (big dish) satellite users are added the numbers increase to 17.3 million households and 45 million users); *see infra* notes 124, 127 and accompanying text.

102 *See* Schaeffler, *supra* note 99.

103 *See id.*

ways. Chiefly, it has created a competitive substitute for cable television.[104] In doing this, it has caused the cable industry to lower its prices and improve its service by adding more channels and converting to digital form.[105] Interestingly, one of the effects of this has been the reduction of the digital divide.[106] In countering one of the strongholds of satellite television,[107] cable companies have begun to tap the resources of rural areas by offering digital cable and Internet access to these areas.[108] This competition is fostering technological development, which increases the quality of the television and will bring forth the aspiration of efficiently merging television with the Internet.[109] Clearly, this is supporting positive economic growth and removes a barrier that is a restriction and a serious threat to the objectives of the Information Age.

II. SATELLITE PIRATES

A. *Interception*

The story of satellite television piracy began with an innocent and legitimate scientific experiment.[110] In 1976, H. Taylor Howard, now considered the 'father of the satellite television industry,' built the first backyard satellite system by using a homemade dish, a converter, and a television set.[111] This system intercepted HBO's signal and began the home satellite television industry.[112] It is important to note that Howard was not a pirate; in fact, after intercepting HBO's signal, he sent the company a check to reimburse it.[113] However, HBO returned Howard's money — someone in their organization did not realize that their industry had just changed.[114] Recalling Howard's experiment and important contri-

104 *See* Geraldine Fabrikant, *One Challenger to Cable TV Fades as Another Appears Via Satellite*, N.Y. TIMES, Jan. 2, 1997, at C14.

105 *See* Fabrikant & Schiesel, *supra* note 92, at C1.

106 *See generally* Fabrikant & Schiesel, *supra* note 92, at C1. The digital divide is a term that is mainly used to describe the socioeconomic dichotomy between those who have access to digital technology, especially the Internet, and those that do not. *See, e.g.*, B. Keith Fulton, *Extending Internet Benefits to All*, 20 CARDOZO ARTS & ENT L.J. 181, 181 (2002).

107 *See supra* note 92 and accompanying text.

108 *See* Fabrikant & Schiesel, *supra* note 92, at C1.

109 *See* Amy Harmon & Jennifer Lee, *Deal Bolsters Satellites as Cable TV Competitors*, N.Y. TIMES, Dec. 17, 2001, at A16.

110 *See* DeBaun, *supra* note 81, at 445; Paul Dykewicz, *Industry Executives Mourn Death of Satellite TV Pioneer*, SATELLITE NEWS, Nov. 18, 2002.

111 *See* DeBaun, *supra* note 81, at 445; Dykewicz, *supra* note 110 ("He was an innovator and an active leader in the satellite television industry for decades . . . [he] had a tremendous impact on the satellite community and gave back to it through the T. Howard Foundation and other endeavors.").

112 *See* Dykewicz, *supra* note 110.

113 *See id.*

114 *See id.*

bution to the industry shortly after his recent death, an executive from one of the industries leaders, EchoStar, noted: "The satellite TV industry wouldn't be where it is today without his vision and his very generous personal contributions over the years . . . . Every dish we install will be a constant reminder of his continued legacy." Nevertheless, there is a dark side to Howard's achievement; it taught people the lesson that satellite signals are vulnerable and can be pirated with a blend of experimentation, intelligence, and malevolence.

B. *Widespread Piracy*

Like Howard, many individuals used home satellite systems to legally intercept television signals.[115] However, this utopia for satellite television viewers did not last.[116] In October of 1984, Congress passed the Cable Communications Policy Act[117] that made it illegal to circumvent the encryption or technological protective measures ("TPMs") that the industry used to scramble satellite signals.[118] However, this law did not criminalize all unauthorized uses of the signals.[119] The interception of unprotected and unscrambled signals was still legal — the law only criminalized the act of willfully circumventing the TPM attached to the programming.[120] Clearly, the law encouraged the satellite television industry to encrypt their programming.[121] Part III will provide an in depth analysis of the laws that support this approach.[122]

Despite criminalizing the theft of satellite signals, the pirates cannot be dissuaded; the lure of the treasure, "free" and unlimited television access seems too fantastic for them to resist.[123] The satellite television industry and the pirates that raid them have a paradoxical relationship — as the industry grows and improves, so does the number of pirates and the effectiveness of their techniques.[124]

---

115 *See* DeBaun, *supra* note 81, at 445–46.

116 *See* 47 U.S.C. § 605 (Supp. III 1985) (amending 47 U.S.C. § 605 (1982)); DeBaun, *supra* note 81, at 446.

117 *See* DeBaun, *supra* note 81, at 446.

118 *See id.* 47 U.S.C. § 605 (1984) ("No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized by law.").

119 *See* DeBaun, *supra* note 81, at 446.

120 *Id.*; California Satellite Systems v. Seimon, 767 F.2d 1364 (9th Cir. 1995).

121 *See, e.g., Seimon*, 767 F.2d at 1364.

122 *See infra* Part III.C–D.

123 *See* Julian Beltrame, *I Want My Satellite TV*, MACLEAN'S, June 10, 2002, at 44; David Lieberman, *Millions of Pirates are Plundering Satellite TV*, USA TODAY, Dec. 2, 2002, at 1A, *available at* http://usatoday.com/news/acovmon.htm (last visited Aug. 30, 2004).

124 *See Helius Developing What it Says is Pirate-Proof Software System*, SATELLITE WK., July 1, 2002.

Evidencing this is the fact that piracy has increased at an alarming rate since the introduction of small dish technology in 1994.[125] As previously noted, the availability of small dish technology and service is responsible for the boom in satellite television, and is the most economically successful faction of the satellite industry.[126] At the end of 2002, there were more than eighteen million satellite television service subscribers in the United States, 2.3 million more than at the end of 2001.[127]

However, there is an additional one to three million people who are pirating satellite television, costing the industry four billion dollars in lost revenue annually.[128] For example, it is estimated that about 1.5 million people pirate DirecTV's service, which costs the company more than one billion dollars in lost revenue annually.[129] The company spent an additional $25 million in developing a new access card with the hope of foiling the pirates and preventing piracy from growing.[130] DirecTV will spend millions of dollars mailing these new access cards to their eleven million paying customers.[131]

C. *The Pathology of Satellite Piracy*

Satellite pirates are a complex breed of white collar criminals. The simple diagnosis for both their addiction to piracy[132] and the overall dilemma would consist of a strict monetary analysis; however, an accurate study of the problem is much more involved.[133] Of course, money and greed serve as great motivating factors for this crime.[134] The crime can be very lucrative; one small ring of pirates made more than $3.2 million in sales from late 1999 to

---

125 *See Satellite Theft*, ELECTRONICS NOW, Jan. 1995, at 35 (noting the instant commercial success of small dish technology). Satellite television became more marketable when small dish technology was introduced to the consumer electronic industry.

126 *See supra* notes 69, 70 and 77 and accompanying text.

127 *See* FCC, *Ninth Annual Report on Competition in Video Markets*, Dec. 31, 2002, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-229984A1.pdf (last visited Aug. 30, 2004). *But see* Lieberman, *supra* note 123, at 1A (reporting that there are 19 million satellite television subscribers); *supra* notes 99–100 and accompanying text.

128 *See* David Lieberman, *Feds Enlist Hacker to Foil Piracy Rings*, USA TODAY, Jan. 10, 2003, at 1B, *available at* http://usatoday.com/tech/news/2003-01-09-hackers_x.htm (last visited Aug. 30, 2004).

129 *See id.*

130 *See id.*

131 *See id.*

132 *See* CYBERCRIME, *supra* note 49, at 29–30.

133 *See generally id.*

134 *See, e.g.*, U.S. DEP'T OF JUSTICE, *Smyrna Businessman Pleads Guilty in Satellite Piracy Case*, Feb. 20, 2003, *available at* http://www.cybercrime.gov/tollensonPlea.htm (last visited Apr. 24, 2003) [hereinafter *Smyrna*].

early 2001.[135] Nevertheless, some pirates are driven by more conceptual considerations — their love for hacking, the challenge of cracking codes, and their thirst for outsmarting the industry.[136]

This dichotomy among the pirates can be explained by the fact that they come from a wide range of social and educational backgrounds. Within their ranks are career hackers,[137] Vietnam veterans,[138] owners of sports bars,[139] authorized satellite dealers,[140] satellite industry employees,[141] and millions of average television viewers looking for a free ride to pay television.[142] The characteristics that these pirates share include a savvy intelligence, a willingness to take risks, and an enthusiasm for their crime.[143] Although profit driven hackers may serve as an immediate threat to the satellite industry, their careers in piracy are often short lived. Conversely, hobbyist pirates are in the business for the long term and will continue to support and diffuse the subculture of hacking; indeed, it is their way of life.[144] The various roles that these individuals play in the crime of satellite piracy will be explored in Part II.E.1.

D. *The Tools of the Pirates*

1. Computer & Internet

Computers and, specifically, the Internet are the gateway technologies for satellite piracy.[145] It is on the Internet that pirates can

---

135 *See, e.g., id. But see* O'SULLIVAN, *supra* note 12, at 6 (providing that white collar crimes are committed as a means to an economic end); PLATT, *supra* note 49, at 92 (noting that satellite pirates who research and develop circumvention methods spend hundreds of thousands of dollars to achieve their goals).

136 *See* PLATT, *supra* note 49, at 11, 50 (arguing that pure hackers are the descendents of Yippies and are interested in fighting the establishment and popular concepts of property, but are not driven by making money). Yippies are the product of late 1960s subcultures, intellectual and rebellious college students who were members of Youth International Party and also identified with the pre-established Hippie movement. *See* CYBERCRIME, *supra* note 49, at 6–7; *see also supra* note 49 and accompanying text.

137 *See generally* PLATT, *supra* note 49, at 74–118.

138 *See id.* at 103. This Veteran justifies his practice of piracy by his belief that the airwaves should be free. *Id.*

139 *See Satellite TV*, SATELLITE WK., Dec. 1, 1997.

140 *See* PLATT, *supra* note 49, at 88 ("*The Transponder*, a respected industry journal, [conducted] a four month survey show[ing] that 95 percent of satellite TV dealers were ready and willing to sell illegally modified decoder boards, and 98 percent of them believed that their customers were ready to buy.").

141 *See* Jennifer Lee, *Student Arrested in DirecTv Piracy Case*, N.Y. TIMES, Jan. 3, 2003; *see also* PLATT, *supra* note 49, at 95 (claiming that an agent of the satellite industry leaked the "fix" to its encryption with the intent of increasing the demand for new encryption that it would develop).

142 *See supra* note 128 and accompanying text.

143 *See, e.g.*, CYBERCRIME, *supra* note 49, at 7.

144 *See* Interview with Mr. X, *infra* note 172.

145 *See, e.g.*, PLATT, *supra* note 49, at 74, 79, 116 (1997); TV@Home: DSS Products (pro-

find all the information and tools that they need to pirate satellite television.[146] While computers run programs that decode encryption, format, and upload the access key card used to regulate programming and identify users,[147] the Internet provides the forum for updating the codes and sharing this information.[148] The codes need updating because the satellite industry uses electronic countermeasures ("ECM") that "destroy" the programming of pirated cards.[149] Web forums are a prime example of the importance of the Internet — pirates use these chat rooms to share information and to hone their techniques.[150] The pirates also join pay sites, at costs between $75 and $100 annually, that list the most recent fixes to the encrypted satellite signals.[151]

---

viding package rates for products and services), *at* http://www.tvathome.tv/products.html (last visited Apr. 25, 2003) [hereinafter DSS Products]. Oddly, this site is very open in its purpose to provide its customers with *free* television. In fact, it does not have a legal disclaimer. *See* Appendices A and B (quoting in full two legal disclaimers). Most of these sites claim to only sell the circumvention tools for educational purposes such as "testing." *Id.*; *see also* HuLoaders.com (noting other web sites that sell (or sold) encryption tools), *at* http://www.huloaders.com/disclaimer.php (last visited Apr. 18, 2003) [hereinafter HuLoaders] (hardcopy on file with author). HuLoaders shutdown their Web site on April 24, 2003. *See* HuLoaders, *supra* note 145, *at* http://www.huloaders.com (last visited Apr. 25, 2003). The only information that is now available on their site states:

> As of today (April 24th 2003), regretfully HuLoaders.com has been closed. Our email will be open until April 27/03 to clear up any remaining issues. We will be no longer offering products and services effective immediately. This was done of our own free will due to legal issues. We sincerely apologize for any inconvenience this may cause our previous clients.
>
> HuLoaders.com

Id. (format of quotation altered). Interestingly, this statement does not note the time that the site was shut down. *Id.* I visited HuLoaders.com on April 24, 2003, at approximately 4:30 PM, to review the products that it offered; I wanted to report my findings in Part II.D.2 of this Article. When I visited the site, it was exactly the same site that I visited on April 18, 2003; thus, it was not shut down. I first noticed that this site was deactivated on April 25, 2003. Additionally, on April 24, 2003, I called the customer service number offered on the site posing as an interested customer located in New York State (the company claimed to be located in Canada). During this conversation, I inquired as to whether the company would sell and send illegal encryption hardware to my New York address. The individual I spoke to answered in the affirmative and assured me that I would have the contraband within a week. At no time through the course of this conversation did the individual advise me on the fact that the company was closing its operation. For the record, I had no intention to purchase any of the contraband; this telephone call was made in the office of the ALBANY LAW JOURNAL OF SCIENCE & TECHNOLOGY using an AT&T telephone card. *See also infra* Part III.C.2 (discussing the wire tap law). The pirates' use of the Internet may also provide a way for law enforcement to prosecute them.

146 *See, e.g.*, HuLoaders, *supra* note 145.

147 *See Instructions For HU Card Programmers*, HU-FILES.com, *at* http://www.hu-files.net/tutorial-extreme-hu.html (last visited Apr. 25, 2003) [hereinafter HU-FILES]; *see also* PLATT, *supra* note 49, at 75, 79, 110, 116.

148 *See* PLATT, *supra* note 49, at 117.

149 *See, e.g.*, Peter Jakel, *Shadowy Figures. Shady Business. Confessions of a Content Pirate.*, SATELLITE BROADBAND, July 2001, at 32.

150 *See id.* at 86–87.

151 *See id.* at 86; HuLoaders, *supra* note 145, *at* http://www.ewebcart.com/cgi-bin/cart.pl (last visited Apr. 24, 2003).

2. Electronic Devices — Wiring the Circumvention

The Internet also acts as a super-store for electronic hardware that is used to circumvent the satellite television industry's encryption.[152] Hundreds of web sites sell everything needed to circumvent the industry's encryption.[153] Some of these sites sell the products in package deals that include a service and code update plan.[154] These "package deals" cost between $109 and $400 depending upon the amount of equipment pirates need, the encryption option they choose to employ, and the term of the service plan they opt to purchase.[155] It is important to note that most of this equipment can only provide the "free" programming on one television. Thus, piracy is not a means for achieving free television; in truth, it is an expensive illegal endeavor.[156] Access cards are an obvious example of this expense since they can only be used on one television at a time. These cards come free with a legally purchased satellite dish; they are formatted, made pirate-ready, and sold on pirate web sites for $99 to $150.[157] There is also the expense of updating these cards, which requires constant attention.[158] This impressive mark-up, coupled with the constant need for updating the equipment and the popularity of piracy, serve to make satellite piracy a billion dollar a year industry.[159]

E. *Inefficiency — How the Pirates Make Their Loot*

The entire underground of satellite piracy — with the notable exception of the end user — benefits from the inefficient nature of its work. Ironically, it also benefits from the continuous technological efforts of the legitimate satellite industry to foil its schemes. Each time the industry changes their access codes or creates a more secure platform for their encryption, the hardened pirate

---

152 *See* DSS Products, *supra* note 145; *see, e.g.*, Incredible DSS, *at* http://www.incredibledss.ca (last visited Sept. 1, 2004) [hereinafter Incredible DSS].

153 *See* Pirates Den (providing an extensive link page to sites that sell circumvention tools), *at* www.pirateden.com (last visited Apr. 25, 2003).

154 *See, e.g.*, DSS Products, *supra* note 145.

155 *See, e.g., id.*

156 *See Six Things You Need to Know About Satellite Television Piracy*, SCRAMBLING NEWS, ¶ 3 (noting that on the average satellite piracy is more expensive than a legal subscription), *at* http://www.scramblingnews.com/piracyfaq.htm (last visited Sept. 1, 2004). *Contra* Jakel, *supra* note 149, at 32 (interviewing a pirate that claims that satellite piracy is less expensive than a legitimate subscription).

157 *Compare* Hucards.com (advertising the sale price), *at* http://www.hucards.com (last visited Sept. 1, 2004) *with* Incredible DSS, *supra* note 152 (selling the card at a "standard rate").

158 *See supra* note 149 and accompanying text; *infra* notes 179–80 and accompanying text.

159 *See* PLATT, *supra* note 49, at 79, 116.

cashes in. Oddly, it is when the "fix" set by the pirate fails that its business propels into a boom market. In fact, pirates have as many as three million customers at the mercy of their next scheme.[160] Only in the perverted world of crime could such an awkward model for generating profit work.[161]

1. The Roles of the Pirates

a. The Learned Hacker

To understand the dynamics of this odd phenomenon, closer attention must be paid to the hierarchy of satellite piracy. Without question, the "Godfather" of the satellite underworld is the learned hacker.[162] It seems fitting that those who are considered to be the proverbial albatross around the neck of the Information Age control their own motives with information. These individuals are the prime mover of satellite piracy; the information they gain by cracking the codes of encryption and the tools they build or reverse engineer are needed in order for satellite piracy to exist.[163] Of course, their skills are most valuable when the legitimate satellite industry changes their encryption; in fact, the industry is static without them.[164]

b. The Entrepreneur — Wholesalers

The other major player in this crime is the information and equipment wholesaler.[165] These pirates invest in the efforts of the learned hacker and market their information and tools.[166] These are also the true risk takers in the underworld of satellite piracy. Where the learned hacker is free to work in solitude and the other players can choose with whom they fraternize,[167] the wholesaler must operate in plain view.[168] Accordingly, they openly market and sell their goods and services illegally, or *quasi*-legally (many of these web sites claim to be based in jurisdictions where the law is not clear) on the Internet.[169] Nevertheless, these pirates are re-

---

160 *See supra* note 128 and accompanying text.

161 Indeed, when viewing satellite piracy from this perspective, one can characterize it as a scheme to defraud. *See infra* notes 324–25 and accompanying text; *see* Part III.E.4 *infra* (discussing the fraud requirement of the mail and wire fraud statutes).

162 *See* CYBERCRIME, *supra* note 49, at 6–7; *see generally* PLATT, *supra* note 49, at 74–118.

163 *See* PLATT, *supra* note 49, at 92.

164 *See supra* notes 149, 160 and accompanying text.

165 *See* CYBERCRIME, *supra* note 49, at 7; DSS Products, *supra* note 145.

166 *See id.*

167 *See infra* notes 174–75 and accompanying text.

168 *See, e.g.*, DSS Products, *supra* note 145.

169 *See, e.g., id.* (claiming, as most of these sites do, that they are based in Canada).

warded for their risk with high profits.[170] These profits are also ignited when the products they sell are rendered obsolete by ECMs; they have an instant market that needs their goods and services.[171]

c. The Card Cleaner

Within this category lies the greatest diversity in motive and level of involvement.[172] Although all of these pirates make the initial investments of equipment, codes, and learning the requisite skills of the trade, the scope of their risk is dictated by their greed.[173] Some of these pirates are *mere* hobbyist thieves — they will only fix cards for themselves and their closest friends.[174] Conversely, there are plenty of pirates who fall within the category of those driven by visions of fast and easy money and who are willing to take greater risks.[175] Some of these individuals make piracy a side job, dealing with acquaintances;[176] others have turned it into a cottage industry.[177] One unscientific study suggests that the authorized dealers of satellite dishes have been practicing this breadth of satellite piracy.[178] Common sense would seem to dictate this: at this stage of our nation's information revolution, it is difficult to believe that there are three million people capable of

---

170 *See e.g., supra* note 135 and accompanying text.

171 *See supra* note 160 and accompanying text.

172 Telephone Interview with "Mr. X," Anonymous Satellite Pirate (Mar. 8, 2003) [hereinafter Interview with Mr. X]. "Mr. X" claimed to be a hobbyist pirate who would only program cards for people that he knew and trusted. *Id.* I have never met, in person, "Mr. X," or any of the other satellite pirates that I have interviewed for the purpose of this Article, nor do I have any knowledge concerning their identity or their personal information. A friend who knew I was researching this issue expressed interest in this Article and was kind enough to arrange for these individuals to contact me via telephone. These individuals contacted me by telephone in the offices of the ALBANY LAW JOURNAL OF SCIENCE & TECHNOLOGY. Before speaking to these pirates, I conducted ample research and prepared test questions to be sure that I was speaking to seasoned pirates. The responses that I received to my questions give me reason to believe that these pirates were being truthful. Moreover, the content of these interviews was of an academic conversation; specifically, I offered no advice or opinions to any of these individuals. Finally, I am operating under the assumption that all of the pirates that I interviewed are located in the Upstate New York area as they expressed. Some of the particular practices of satellite piracy, such as their rates and fee arrangements, may differ according to geographic considerations.

173 *Id.*; Telephone Interview with "Mr. Y," Anonymous Satellite Pirate (Mar. 14, 2003) [hereinafter Interview with Mr. Y]. "Mr. Y" claimed to program cards for approximately forty end users.

174 Interview with Mr. X, *supra* note 172.

175 *Id.*

176 Interview with Mr. Y, *supra* note 173.

177 *Id.*; *see supra* note 139 and accompanying text.

178 *See supra* note 139 and accompanying text; Interview with Mr. X, *supra* note 172 (noting a "brave" pirate that ran his illegal business in a Radio Shack store located in a shopping mall).

cracking strong encryption — even if there are step-by-step directions on the Internet.

Parallel to this consideration is the demand for this service that these pirates provide. The service they offer has two prongs: (1) they introduce end users into the world of pirated television, frequently purchasing the circumvention tools the end user may need; and (2) they clean and update their access cards when the satellite industry transmits ECMs.[179] Like the other players in this crime, these pirates benefit from the legitimate satellite industry updating their encryption. Each time an end user's card needs to be cleaned or updated, the card cleaner makes money;[180] however, the more "benevolent" among them charge a flat monthly rate that is not affected by the number of times updating is required.[181]

d. The End User

The end user — the personal home user — is the consumer in the underworld of satellite piracy. Without them, widespread satellite piracy would not exist. Indeed, they are active consumers who take part in the illegal activity.[182] In short, they demand the knowledge and services of the other players in this crime. However, like the other players, they also contribute in defrauding the satellite industry.[183] For example, they do this by lying to the retailer about the use of the satellite system,[184] by not installing the satellite system properly,[185] and by having the industry's access card illegally programmed.[186]

Nevertheless, end users seem to have simplistic motivations,

---

179 Interview with Mr. Y, *supra* note 173.

180 *See supra* note 160 and accompanying text.

181 Interview with Mr. Y, *supra* note 173. However, the price for this flat fee arrangement may be highly inflated. *Id.*

182 *See id.*

183 *See supra* notes 163, 164 and 171, and accompanying text.

184 Interview with Mr. X, *supra* note 172 (stating that many end users provide false personal information when purchasing satellite systems from retailers such as Radio Shack); *see, e.g.*, United States v. Manzer, 69 F.3d 222, 226 (8th Cir.1995) (holding that the defendant's satellite piracy scheme was fraudulent). *But see infra* note 437 and accompanying text. Here, it is important to note that the defendant in *Manzer* was not an end user, but a wholesaler. *See Manzer*, 69 F.3d at 225.

185 Interview with Mr. X, *supra* note 172. A properly installed home satellite system includes the use of the homeowner's telephone lines so they can properly order pay-per-view programs and so the satellite provider can track the customer's billing. *Id.* End users, however, install the satellite system without jacking it into their telephone line. *Id.* Therefore, they do not activate their account or notify the provider that they own one of their systems. *Id.*

186 *See* Interview with Mr. Y, *supra* note 173. The type of circumvention employed in satellite piracy can be characterized as a fraud since it is sending a false signal (a fraudulent communication) to the satellite provider. *Id.* This false signal permits the end user to view the otherwise protected television programming. *Id.*

the fantasy of unlimited access to "free" television.[187] As one commentator has noted, "[o]ur motivation is a natural inclination toward saving money and to get better TV in our homes."[188] In spite of this, end users take considerable risks that are more tangible than fraud in their attempts to pirate satellite television and are most likely unaware of the consequences. As noted, all end users possess an illegally programmed access card that is designed to circumvent encryption and install a satellite dish on the roof of their homes that is not authorized to receive service.[189] Depending upon the approach to piracy employed by the end user, they may also possess additional circumvention tools that the law has deemed contraband.[190]

As a class, these pirates are perceived as the least knowledgeable and the most vulnerable to exploitation.[191] End users must depend upon the honesty of individuals and bear the cost of inefficiency that the more involved pirates enjoy. Their role in satellite piracy is also one of an illogical dependency. They must trust the other pirates who can control, through programming, when their services will be needed.[192]

F. *White Collar Pirates*

In spite of their variances in philosophy and appearance,[193] nearly all satellite pirates are white collar criminals. Practicing satellite piracy requires education, a thorough understanding of complex interactions, honed problem-solving skills, a financial investment, and the ability to circumvent encryption.[194] Moreover, satellite pirates are nonviolent and goal oriented criminals.[195] As will be explained in Part II.G below, the consequence of the crime of satellite piracy, like most other white collar crimes, is chiefly economic and is based on fraud.[196] Satellite pirates share other simi-

---

187 Jakel, *supra* note 149, at 32.

188 *Id.*

189 Interview with Mr. Y, *supra* note 173.

190 17 U.S.C. § 1201. *See* Andrew Harris, *Suit Accuses DirecTV of Dishing it Out*, NAT'L L.J., *available at* http://www.nlj.com/business/120902ledebiz.shtml (last visited Apr. 25, 2003); Interview with Mr. X, *supra* note 172.

191 *See supra* notes 164, 171, and 179–81, and accompanying text.

192 *See* Interview with Mr. Y, *supra* note 173.

193 *See supra* note 2 and accompanying text.

194 *See generally* PLATT, *supra* note 49, at 74–118. *See also supra* note 13 and accompanying text (noting that circumvention is included in the definition of white collar crimes).

195 *Compare id.* at 101 (noting that satellite piracy does not include the use of violence or even threats), *with* O'SULLIVAN, *supra* note 12, at 5 (noting that white collar crimes are limited to crimes that do not use violence or even threats).

196 *Compare id.* at 79, *with* O'SULLIVAN, *supra* note 12, at 5. *See also supra* notes 128–31 and 134, and accompanying text.

larities to traditional white collar criminals: they scare easily when they are confronted by the law and they are valuable to law enforcement agents.[197] Law enforcement agents are often interested in using them to prosecute other pirates and to gain insight into how the culture of their niche in the criminal world operates.[198]

G. *The Negative Impact of Satellite Piracy*

1. Negative Economic Impact

Like other white collar crimes,[199] the primary negative social impact of satellite piracy is economic loss and inefficiency.[200] The lost profits[201] and expenditures on research and development tools to limit piracy[202] are unfortunate losses of revenue and an inefficient allocation of resources. To reiterate, the satellite television industry loses over four billion dollars annually in revenue due to piracy.[203] The immediate effect of this is a higher price that legitimate consumers must pay.[204] Further, it would be naive to believe that satellite piracy only affects the legitimate satellite industry.[205] Each individual that pirates satellite television access cards is also pirating pay-per-view events, movies, sporting events, and "cable" channels.[206] Therefore, not only are pirates circumventing encryption, they are also bypassing the need to rent a movie from Blockbuster and the fee to access all of the NFL's televised games.[207] Every piece of intellectual property transmitted via satellite television is made vulnerable by satellite piracy and is losing profits because of it. This is dangerous to the development of the

197 *See* Lisa Sink, *Felony Charge Dismissed in Satellite TV Piracy Case*, MILWAUKEE J. SENTINEL, June 15, 2002, at 03B (noting the remarks of one pirate's attorney who characterized the pirate as one of the most frightened clients he has had).

198 *See* Lieberman, *supra* note 128, at 1B (reporting the arrest and plea deal of Steven Woida, a.k.a. Steve Frazier; it is believed that certain individuals from Afghanistan were also interested in his hacking services following September 11, 2001); *see also* O'SULLIVAN, *supra* note 12, at 985–86 (addressing white collar cooperation agreements).

199 The most notable exception is environmental crimes prosecuted under the "public welfare" or "responsible corporate officer" theories. The negative impact of environmental crimes is two-tiered in that they negatively affect the economy and create the more tangible injury of pollution. *See, e.g.*, O'SULLIVAN, *supra* note 12, at 75–86, 187–91.

200 *See supra* notes 128–31 and accompanying text.

201 *See supra* notes 128–29 and accompanying text.

202 *See supra* notes 130–31 and accompanying text.

203 *See supra* note 128 and accompanying text.

204 *See* Ellen McCarthy, *A New Focus on Movie Piracy: Battling Bootleggers With Distortion*, WASH. POST, Oct. 14, 2002, at E05.

205 *See, e.g.*, Michael Arnone, *Privacy Under Assault: Can Encryption Prevent Piracy Without Harming the Consumer?*, TELEVISION Q., Fall 2001, at 38 (discussing the problem of easy copying that exists with digital technologies). Strong encryption was demanded in satellite television by the movie studios and the broadcast networks. *See id.*

206 *See id.*

207 *See id.*

Information Age; thus, it is precarious to today's economy. In 2001, the intellectual property transmitted on satellite television was worth $457.2 billion, or five percent of the National Gross Domestic Product.[208]

2. Negative Social Impact

Satellite piracy is a unique white collar crime since it seems to be socially accepted. The popularity of the crime supports this theory.[209] Congress, the courts, and certain elements of law enforcement perpetuate this sentiment by not taking an interest in investigating or prosecuting satellite piracy.[210] Therefore, it will take more than improved encryption and ECMs to limit this crime. The satellite industry and law enforcement will have to change society's perception that this form of piracy is an innocent theft. Changing this perception will also aid in the development of the Information Age by making society aware of the importance of protecting and respecting intellectual property.[211] Part IV will illustrate that the laws needed to change society's perception of satellite piracy are not firmly in place and are not available to readily prosecute and punish every class of pirate.[212]

III. Laws Applicable to Prosecuting Satellite Pirates

When analyzing the crime of satellite piracy, it is necessary to first discriminate between the pirates and then to analyze their culpability and their criminal liability accordingly. For this purpose, the distinctions among satellite pirates made in Part II.E — learned hackers, wholesalers, card cleaners, and end users — are especially useful. This Part will analyze various laws that are and can be useful in prosecuting satellite piracy. In doing this, this Part will consider how the law applies to each player in this crime and will draw general conclusions concerning the pirates' civil and criminal liability. The legal analysis presented will illustrate that there is a need for a law that creates clear and stiff penalties for end users to deter the commission of this crime.

A. *A Brief Study of Criminal Copyright Law*

A prerequisite to a thoughtful study of the laws that criminal-

---

208 *See id.* at 40.
209 *See supra* note 128 and accompanying text.
210 *See* 47 U.S.C. § 605(d)(5) (2001); Dowling v. United States, 473 U.S. 207 (1985); Lieberman, *supra* note 123, at 1A.
211 *See supra* note 197 and accompanying text.
212 *See supra* Part IV.

ize satellite piracy is a basic understanding of criminal copyright law. This understanding must include two old concepts that once served as the bedrock of criminalizing copyright violations. First, "[s]ince 1897, when criminal copyright infringement was introduced into U.S. copyright law the concept differentiating criminal from civil copyright violations has been that the infringement must be pursued for purposes of commercial exploitation."[213] The second of these principles is similar to the first and was also initiated in 1897; it identifies the *mens rea* "as conduct that is 'willfull' [sic] and undertaken 'for profit.'"[214]

In 1976, Congress drastically revised the copyright law and "eased" the *mens rea* requirement by deleting the "for profit" standard and inserting "willfully and for purposes of commercial advantage or private financial gain."[215] In 1982, Congress made certain cases of copyright infringement a felony, but did not alter the *mens rea* standard set forth in 1976.[216] Finally, in 1997, following the disturbing *United States v. LaMacchia* case,[217] Congress passed the No Electronic Theft ("NET") Act.[218] The passage of the NET Act also marked the beginning of Congress's drastic alterations to copyright law that shifted copyright's balance in the favor of copyright holders, but failed to provide a solution to widespread piracy.[219]

---

213 United States v. LaMacchia, 871 F. Supp. 535, 539 (D. Mass. 1994) (citations omitted).

214 *Id.* Identifying what "willful" means is difficult. *See* Spies v. United States, 317 U.S. 492, 497 (1943) ("[W]illful . . . is a word of many meanings, its construction often being influenced by its context."). For a full discussion on the complexity of understanding the mental state of "willful," *see* Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and The Importance of the Willfulness Requirement*, 77 WASH. U. L.Q. 835, 879 (1999) *and* U.S. DEP'T OF JUSTICE, *Computer Crime and Intellectual Property Section*, ¶ B.3, *at* http://www.usdoj.gov/criminal/cybercrime/ipmanual/03ipma.htm#III.B.3 (last visited Aug. 30, 2004) [hereinafter *Computer Crime*].

215 *LaMacchia*, 871 F. Supp. at 539 (quoting 17 U.S.C. § 506(a)). This language has caused confusion and has allowed some intellectual property pirates to avoid maximum liability. *See id.*

216 *See id.* at 539–40.

217 *Id.*; *see also infra* notes 361–432 and accompanying text (discussing the *LaMacchia* holding and the precedent it relied on).

218 No Electronic Theft ("NET") Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997). *See infra* notes 231–37 (discussing the NET Act).

219 *See* Wendy M. Grossman, *Cyber View: Downloading as a Crime*, SCI. AM., Mar. 1998, at 37 (noting that the NET Act fails to provide fair-use exemptions). *See generally* David V. Lampman, II, Comment, *"A Prologue to a Farce or a Tragedy"? A Paradox, a Potential Clash: Digital Pirates, The Digital Millennium Copyright Act, The First Amendment & Fair Use*, 38 GONZ. L. REV. 367 (2003) (discussing how the Copyright Term Extension Act and the Digital Millennium Copyright Act contribute to copyright law heavily favoring copyright holders at the expense of society's interest in access and fair use).

1. Basic Criminal Penalties under the Copyright Act of 1976

Section 506 of the Copyright Act of 1976 and 18 U.S.C. § 2319 address the basic criminal penalties for copyright infringement.[220] A first offense of copyright infringement is generally punishable with a maximum of five years imprisonment.[221] A second offense generally carries a maximum term of ten years imprisonment.[222] Additionally, if a person is found guilty of violating this provision, the court may order forfeiture of all the tools used in connection with the infringement.[223]

2. Basic Civil Remedies under the Copyright Act of 1976

Section 504 of the Copyright Act of 1976 addresses civil remedies for copyright infringement.[224] The civil remedies offered to the copyright holder include temporary and permanent injunctive relief, actual damages and any profits made in connection with the infringement, and an option for statutory damages.[225] The statutory damages range from $750 to $30,000 for each act of infringement.[226] If the copyright holder can prove a willful infringement, statutory damages are available up to $150,000.[227]

Since the last major alterations of the criminal copyright law, society has again changed[228] and has become more dependent upon intellectual property — the logic behind these laws predates or arose at the inception of the Information Age. Moreover, they are extremely difficult to use since they require a showing of actual infringement.[229] Nevertheless, updating these principles of criminal copyright law with penalties that will serve to deter piracy has been difficult.[230] The consequence of this slow and awkward development is the use of criminal copyright standards that are not apt to deter those who drive the demand for satellite piracy — the end users. As will be explained, perhaps Congress failed to foresee the need to punish end users.

---

220 17 U.S.C. § 506 (2001).
221 18 U.S.C. § 2319(b)(1) (2001).
222 *Id.* at (b)(2).
223 17 U.S.C. § 506(b).
224 17 U.S.C. § 504(a) (2001).
225 *Id.* at (a) – (c).
226 *Id.* at (c)(1).
227 *Id.* at (c)(2).
228 For example, the Internet and other digital forms of media have made copyright infringement efficient because digital copies do not decrease in quality as analogue copies do. Moreover, this change in technology has afforded new opportunities for infringement such as file-to-file "sharing."
229 *See supra* note 220 and accompanying text.
230 *See, e.g., LaMacchia*, 871 F. Supp. at 545 (refusing to extend the wire fraud statute to a computer hacking crime).

B. *The No Electronic Theft ("NET") Act*

The NET Act amended criminal copyright statutes by eliminating the financial gain prerequisite and by making it illegal to reproduce or distribute copyrighted materials.[231] The NET Act did this by altering the definition of "financial gain" in 17 U.S.C. § 101 to include the receipt of copyrighted material.[232] Under the NET Act, the government only needs to prove that the infringer acted for financial gain, or that he/she reproduced or distributed one or more copies of protected works that have a total retail value of $1000.[233] Therefore, because of the NET Act, the criminal copyright statute now reaches infringers who act solely to harm another without the goal of a financial gain. Ironically, by passing the NET Act, Congress eliminated the *mens rea* requirements that initially justified criminalizing copyright infringement.[234]

By passing the NET Act, however, Congress did not provide a viable means to thwart or even deter all types of intellectual property piracy. This conclusion is based upon the fact that the scope of the NET Act does not extend to all criminal statutes that include the phrase "private financial gain" and that refer to intellectual property.[235] Furthermore, the NET Act specifically amends the phrase "private financial gain" in the definition section of the Copyright Act, 17 U.S.C. § 101.[236] In fact, the NET Act only references sections of 17 U.S.C. § 506 and 18 U.S.C. § 2319.[237]

C. *Laws Specifically Criminalizing Satellite Piracy*

1. 47 U.S.C. § 605 — The Cable Communications Policy Act

As previously noted in Part II.B, in October of 1984, Congress passed the Cable Communications Policy Act, which criminalized the circumvention of the encryption that the satellite industry used to scramble their signals.[238] By passing this law, Congress amended the Federal Communications Act of 1934, and encouraged a mar-

---

231 *See, e.g.*, Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 249 (1999).

232 No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997).

233 *Id.* at § 2(a).

234 *See supra* note 213–14 and accompanying text.

235 *See infra* notes 257–60 and accompanying text.

236 No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 § 2(a) (1997).

237 *See id.*

238 *See* 47 U.S.C. § 605 (2001) ("No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized by law."); Time Warner Cable v. Dockins, 96 Civ. 6852 at *9 (S.D.N.Y. 1998) (noting that 47 U.S.C. § 553 and 47 U.S.C. § 605 are similar statutes), 1998 U.S. Dist. LEXIS 22689. The main difference is that 47 U.S.C. § 553 applies to cable television and 47 U.S.C. § 605 applies to satellite television. *See* DeBaun, *supra* note 81, at 446.

ket solution to "piracy" by promoting the use of self-help remedies, such as encryption.[239] This is evidenced by the fact that the law did not criminalize all unauthorized use of the signals.[240] The interception on unprotected and unscrambled signals was still legal.[241]

a. Civil Remedies

By passing this law, Congress created a cause of action for civil remedies and criminal penalties for satellite piracy violations.[242] The civil remedies include injunctive relief, actual damages, statutory damages, and attorney's fees to the prevailing party.[243] The statutory damages for a willful violation range from $1000 to $10,000.[244] If the violation is committed willfully and for purposes of direct or indirect commercial advantage or private financial gain, damages could be awarded up to $100,000.[245] Additionally, there is a similar increase in civil damages, up to $100,000, for an individual who manufactures, sells, or modifies equipment, "*knowing* or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services."[246]

b. Criminal Penalties

The criminal penalties for a willful violation of this law include a fine not to exceed $2000 and up to six months imprisonment.[247]

---

239 *See* DeBaun, *supra* note 81, at 446, 459–60 (noting that the government wanted to limit their involvement in regulating satellite piracy).

240 *See id.*

241 *See* California Satellite Systems v. Seimon, 767 F.2d 1364 (9th Cir. 1995); *id.*

242 47 U.S.C. § 605(e) (2001).

243 *Id.* at (e)(3)(B)(i–iii).

244 *Id.* at (3)(C)(i)(II); *see, e.g.*, DirecTv v. Disalvatore, 2003 U.S. Dist. LEXIS 23822, at *19 - *24 (N.D. Ohio May 21, 2003), *available at* http://www.hackhu.com/Order%20Granting%20Summary%20Judgment.pdf (last visited Aug. 30, 2004). In *Disalvatore*, DirecTv moved for summary judgment against four defendants claiming that they violated 47 U.S.C. § 605, 18 U.S.C. §§ 2510-2221, along with state laws. *Id.* at *3. DirecTv filed the claim in April of 2002 and initially named twenty-three defendants. *Id.* at *3. DirecTv argued that the defendant's violated these laws by purchasing and using encryption devices to surreptitiously intercept their programming. *Id.* It is interesting to note that each of the four defendants that were named in this action were apprehended after purchasing encryption devices over the Internet — law enforcement agents were able to track the defendants' purchases through their credit card information. *Id.* at *4. Moreover, each of the named defendants was charged with using "extra" tools to circumvent DirecTv's encryption, beyond a naked programmed access card. *Id.* at *4-7. In fact, and as mentioned, these tools lead law enforcement to the defendants. *See id.* at *4. In granting DirecTv's motion for summary judgment, the court awarded them $10,000 against each defendant along with attorney's fees and costs. *Id.* at *20-23. The court, however, did not note under which claim it was awarding the damages. *Id.* at *20-24.

245 47 U.S.C. § 605(3)(C)(i)(II) (2001).

246 *Id.* at (e)(4), (3)(C)(II)(ii) (emphasis added).

247 47 U.S.C. § 605(e)(1) (2001).

If the violation was done willfully with purposes of direct or indirect commercial advantage or private financial gain, the fine is increased to $50,000 and/or up to two years imprisonment.[248] Repeat offenders could be fined up to $100,000 and/or imprisoned for up to five years.[249] Those who manufacture, distribute, or modify equipment can be fined up to $500,000 for each violation and/or imprisoned up to five years.[250]

This law's stiffest penalties would apply to hackers because they manufacture or at least modify equipment (by applying the hacked code), to wholesalers because they sell the equipment, and to card cleaners because they modify (by updating the codes) or assemble the intricate circumvention equipment for their customers.[251] These individuals are liable for up to $100,000 in civil statutory damages[252] and are criminally liable for up to $500,000 and/or a maximum of five years imprisonment.[253]

Conversely, when applied to end users, the statutory damages and criminal penalties of this law are too menial. The explanation for this is relatively simple; Congress drafted the statute to exclude end users from its utmost liability.[254] The statute states that ". . . the term 'private financial gain' shall not include the gain resulting to any individual for the private use in such individual's dwelling unit of any programming for which the individual has not obtained authorization for that use. . ."[255] Therefore, it seems that the minimal criminal penalties of $2000 and up to six months imprisonment are the only penalties applicable to end users under this law.[256] Since this law requires a mental state unfit to prosecute all satellite pirates to the fullest extent of the law, prosecutors must look to other laws that appropriately penalize these criminals.

---

248 *Id.* at § 605(e)(2).

249 *Id.*

250 *Id.* at § 605(e)(4).

251 *Id.*; *see also* Part II.E.a–c.

252 47 U.S.C. § 605(3)(C)(II)(2001).

253 *Id.* at § (e)(4).

254 *See* Time Warner Cable v. Dockins, 96 Civ. 6852 (S.D.N.Y. 1998), 1998 U.S. Dist. LEXIS 22689; *see also infra* note 263 and accompanying text. Even if Congress wanted to expand the scope of the phrase "willfully and for the purpose of commercial advantage or private financial gain" it would not fit when applied to end users. End users pirate satellite signals willfully; however, they do not do so with the purposes of direct or indirect commercial advantage or private financial gain. End users may save money by bypassing an expense — this does not account for a private financial gain. As previously noted, these pirates may be better off financially if they legitimately subscribed to satellite television. *See supra* note 156.

255 47 U.S.C. § 605(d)(5) (2001).

256 *Id.* at § 605(e)(1).

c. The Effect of 47 U.S.C. § 605's End User Exemption on Other Laws

Before analyzing this complex issue, it is important to clearly identify the predicament it creates: Does 47 U.S.C. § 605(d)(5) act as a limiting definition of the phrase "private financial gain" as applied to end users? In other words, does the exemption that Congress created in 47 U.S.C. § 605 apply to all other criminal laws, and thus, prevent end users from making a private financial gain and from being prosecuted under the law's stiffest penalties?

This matter is most interesting when analyzing the specific issues of the NET Act and the Digital Millennium Copyright Act ("DMCA"). As will be explained in Part III.D, the DMCA is rooted in copyright law; consequently, it falls within the scope of the NET Act, which amended the definition of "financial gain" in 17 U.S.C. § 101 to include the receipt of copyrighted material — such as satellite programming — and does not require a profit motive.[257] Therefore, there is a direct conflict between 47 U.S.C. § 605, the law specifically designed to prosecute satellite pirates, and the combination of the NET Act and the DMCA, laws that were designed to purge the Information Age of intellectual property pirates. This conflict creates an intriguing paradox that is particularly material. As noted, an end user's liability under 47 U.S.C. § 605 is slight — a maximum fine of $2000 and up to six months imprisonment.[258] In contrast, if liable under the DMCA, or in other words, if found to have pirated "willfully and for the purpose of commercial advantage or *private financial gain*,"[259] the end user's liability becomes severe — a maximum fine of $500,000 and/or a term of imprisonment up to five years for first time offenders.[260]

The most illustrative and logical commentaries on this type of conflict seem to point in the favor of the end user. For example, the Supreme Court has repeatedly stated that: "[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite."[261] Since 47 U.S.C. § 605 — the law specifically designed to protect satellite signals — exempts end users

---

257 *See infra* notes 276–311 and accompanying text; *see supra* notes 231–37 and accompanying text.

258 *See supra* note 256 and accompanying text.

259 17 U.S.C. § 1203(4) (emphasis added).

260 17 U.S.C. § 1204(a)(1).

261 *Dowling*, 473 U.S. at 215 (quoting United States v. Universal C. I. T. Credit Corp., 344 U.S. 218, 221-222 (1952) (citations omitted)).

from its definition of private financial gain, and accordingly, its most harsh liability, it would seem that Congress intended to protect end users from the most stern penalties. Conversely, the DMCA is a much more general law. In fact, the DMCA does not specifically address the issue of satellite piracy and ignores the issue of private financial gain as applied to end users. Here, it is important to note that in 1998, when the DMCA was passed, satellite piracy was already a booming business that negatively affected the satellite industry. Nevertheless, Congress took no action to amend 47 U.S.C. § 605's end user exemption. Writing for the court in *Time Warner Cable v. Dockins*,[262] a case analyzing 47 U.S.C. § 605(d)(5), Judge Patterson adds support to this reasoning:

> If 'private financial gain' applied to private users of cable descrambling devices, such as [the defendant end user], the term would apply to all users of such devices. If so, the statutory provision requiring proof that the defendant acted for 'private financial gain or commercial advantage' would add nothing to the separate requirement of proof of willfulness, and would thus constitute mere surplusage. Such a result is ordinarily not countenanced.[263]

Therefore, for the criminal law to be consistent and fair on this issue, courts must interpret a Congressional intent to exclude end users from all definitions of private financial gain in light of 47 U.S.C. § 605's end user exemption. This must be the interpretation until Congress clearly amends it.[264]

2. 18 U.S.C. § 2512 — The Wire Tap Law

The Wire Tap Law is an entirely criminal statute that makes it illegal to intentionally possess, assemble, or sell a device that circumvents, unscrambles, or intercepts wire, oral, or electronic communications that have been placed in the mail or stream of interstate or foreign commerce.[265] It is required that this be done with knowledge that the device is primarily useful for circumvention.[266] Tools that unscramble satellite television signals are also prohibited by this law.[267] This law also makes it illegal to advertise

---

262 96 Civ. 6852 (S.D.N.Y. 1998), 1998 U.S. Dist. LEXIS 22689.

263 *Id.* at *13 (criticizing Cablevision Sys. New York City Corp. v. Lokshin, 980 F. Supp. 107, 109, 114 (E.D.N.Y. 1997)). *Lokshin* held that the private use of an unscrambler is a "private financial gain," since the end user "avoids paying otherwise obligatory fees to the cable system operator, she necessarily acts for her own financial gain." *Id.* at *11.

264 *See supra* note 261 and accompanying text.

265 18 U.S.C. § 2512(1)(b) (2001).

266 *Id.*

267 *Id.* Specifically, it is illegal under this statute to mail or transport in interstate or

the sale of such tools.[268] Violations of this law contain a fine of up to $10,000 and/or a maximum prison term of five years.[269] Further, courts have held that forfeiture is proper under this statute.[270] It is interesting to note that in October, 1986, this law was amended by changing the *mens rea* from willful to intentional.[271]

Like the Cable Communications Policy Act, the Wire Tap Law can be used to prosecute hackers, wholesalers, and card cleaners; but the Wire Tap Law falls short in that end users are most likely outside the scope of its most harsh penalties. Hackers are criminally liable because they manufacture or assemble tools used to pirate satellite television.[272] Wholesalers' liability under this law can stem from any of the conduct that it prohibits, such as assembling, possessing, and selling this equipment. They can also be prosecuted under the anti-advertising provision of this statute since they frequently advertise on Internet sites related to satellite piracy.[273] The law applies to card cleaners since they possess tools that are used to clean and program the access cards that unscramble the satellite signal. Further, depending upon the circumvention system used by their "client," card cleaners may assemble the intricate circumvention equipment for their less knowledgeable customers, which are prohibited by this law.

The issue of possession is the key to analyzing end user liability since end users do not typically assemble or sell circumvention tools. There are two factors that must be considered in determining whether an end user is within the scope of this law. First, one must determine if a programmed access card — the same card that was legally issued by the legitimate satellite industry — is an illegal device under this law. If a programmed access card is considered an illegal device, then the end user can be held liable. However, if it is not considered an illegal device proscribed by this law, then the second factor, the system of circumvention, must be analyzed. Although most end users only use a "naked" hacked access card,

---

foreign commerce the circumvention device or any component of the device. *Id; see also* United States v. Harrell, 983 F.2d 36 (5th Cir. 1993) (affirming conviction for the modification and sale of the famous Video-Cipher system); United States v. Lande, 968 F.2d 907 (9th Cir. 1992); United States v. Shriver, 989 F.2d 898 (7th Cir. 1992); United States v. Splawn, 982 F.2d 414 (10th Cir. 1992).

268 18 U.S.C. § 2512(1)(c).

269 *See, e.g.*, United States v. Herring, 993 F.2d 784, 786 (11th Cir. 1993) (affirming the convictions of wholesalers of devices used to pirate satellite television under this provision of the Wire Tap Law).

270 *See, e.g.*, United States v. One Macom Video Cipher II, 985 F.2d 258 (6th Cir. 1993) (holding that the illegal tools were subject to forfeiture under 18 U.S.C. § 2512).

271 *See* P.L. 99-508, Title I, § 101(c)(1), (7), (f)(2), 100 Stat. 1851.

272 *See* United States v. Splawn, 982 F.2d 414; *see also* PLATT, *supra* note 49, at 85.

273 *See, e.g.*, DSS Products, *supra* note 145.

some choose to employ a more advanced strategy for circumvention that includes a plethora of devices that serve to protect the programmed access card against the satellite industry's ECMs.[274] If the end user is utilizing these "extra" tools, then they are in possession of an illegal device and are within the scope of this law.[275]

D. *The Digital Millennium Copyright Act*

The DMCA is the newest law designed to prosecute digital pirates.[276] President Clinton signed the DMCA on October 28, 1998, with the intent of updating the copyright law so it would be consistent with the developments of digital technologies and the Internet.[277] In drafting the DMCA, Congress created the most drastic revision to the Copyright Act of 1976. Unlike traditional copyright laws, the DMCA does not address the act of infringement; rather it concentrates on the technologies that facilitate infringement.[278] Therefore, the holder of a copyright-protected work does not have to prove infringement; she only has to show that the encryption she used to protect the copyrighted work was circumvented.[279]

Section 1201 of the DMCA states that "[n]o person shall circumvent a technological measure that effectively controls access to

---

[274] Interview with Mr. Y, *supra* note 173 (discussing "looping" methods and "emulators" that serve to prevent ECMs from reaching the pirated access card). Mr. Y states that these extra tools are used infrequently because they are more expensive and difficult to install. *Id*; *see* United States v. Lande, 968 F.2d 907 (9th Cir. 1992) (noting that the defendant's encryption device was within the scope of 18 U.S.C. § 2512 because he permanently changed the primary purpose of the satellite industry's unscrambling device by making major modifications to it).

[275] *See supra* note 244 (discussing the *Disalvatore* case and noting that each defendant was found guilty of using "extra" tools to circumvent DirecTv's encryption). Thus, there seems to be no record of judgment being filed against an end user who merely uses a naked programmed card. Indeed, these pirates seem impossible to trace.

[276] *See* Thor Olavsrud, *FBI, DOJ Crack Satellite Piracy Ring*, ESECURITY PLANET, Feb. 11, 2003 (reporting the recent arrests of seventeen satellite pirates), *at* http://www.esecurityplanet.com/views/article.php/1582881 (last visited Sept. 1, 2004).

[277] *See Clinton Statement on the Digital Millennium Copyright Act*, U.S. NEWSWIRE, Oct. 28, 1998, *available at* 1998 WL 13606936. After signing the DMCA, President Clinton stated:

> These treaties will become effective at a time when technological innovations present us with great opportunities for the global distribution of copyrighted works. These same technologies, however, make it possible to pirate copyrighted works on a global scale with a single keystroke. The WIPO treaties set clear and firm standards—obligating signatory countries to provide "adequate legal protection" and "effective legal remedies" against circumvention of certain technologies that copyright owners use to protect their works, and against violation of the integrity of copyright management information. This Act implements those standards, carefully balancing the interests of both copyright owners and users . . . Through enactment of the Digital Millennium Copyright Act, we have done our best to protect from digital piracy the copyright industries that comprise the leading export of the United States.

Id. The DMCA was passed, in part, to comply with the 1996 WIPO treaty.

[278] 17 U.S.C. § 1201(2001).

[279] *See supra* note 220 and accompanying text.

a work protected under this title."[280] It also bans the creation, marketing, and trafficking of devices or services designed to crack encryption technologies and imposes civil and criminal penalties for violations of the section.[281] Any device is illegal under this provision if it "(A) is primarily designed or produced for the purpose of circumventing a technological measure . . . ; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure . . . ; or (C) is marketed for use in circumventing a technological measure . . . ."[282] This provision applies to satellite piracy in that "de-scrambling" a work that is "scrambled" by encryption is a violation that is within the scope of the law.[283]

The DMCA imposes both civil remedies and criminal penalties for violations of section 1201.[284] The civil remedies offered to the copyright holder include temporary and permanent injunctive relief that would reasonably prevent violations of section 1201,[285] actual damages and any profits made in connection with the infringement,[286] and an option for statutory damages.[287] Reasonable attorney's fees and costs may also be awarded to the prevailing party under the discretion of the court.[288] Furthermore, a repeat offender that violates section 1201 within three years of final judgment is subject to treble damages.[289]

I. Criminal DMCA & Satellite Pirates

Prosecution under the criminal penalties of section 1201 of the DMCA requires a person to be found to have violated the section "willfully and for the purpose of commercial advantage or private financial gain."[290] The penalties include a fine that may not exceed $500,000 and/or a term of imprisonment up to five years

280 17 U.S.C. § 1201(a)(1)(A).
281 *See id.* at § 1201(a)(2).
282 *Id.*
283 *Id.* at § 1201(a)(3)(A); Symposium, *Exploring Emerging Issues: New Intellectual Property, Information Technology, and Security in Borderlesss Commerce: The Anti-Circumvention Provision of The Digital Millennium Copyright Act*, 8 TEX. WESLEYAN L. REV. 593, 597 and n.18 (2002) ("The legislative history of this section indicates that Congress modeled this provision after existing laws banning 'black boxes,' which function to descramble cable-television and satellite-cable services.") (citing H.R. Rep. No. 105-551, pt. 2, at 38 n.2 (1998)).
284 *See* 17 U.S.C. § 1203 (providing civil remedies); 17 U.S.C. § 1204 (creating criminal penalties).
285 17 U.S.C. § 1203(b)(1). The court may also impound any product in the control of the alleged infringer that they have reasonable cause to believe was used in connection to the violation. *Id.* at (b)(2).
286 *Id.* at (b)(2).
287 *Id.* at (b)(3). The court has discretion to award no less than $200 and no more than $2500 per violation. *Id.*
288 17 U.S.C. § 1203(b)(6).
289 17 U.S.C. § 1203(4).
290 17 U.S.C. § 1204(a).

for first time offenders.[291] The fine and term of imprisonment are doubled for subsequent offenders.[292] Further, under this law a defendant may incur civil and criminal liability for the same act of circumvention.[293] There is a five-year statute of limitations on this crime.[294]

a. Circumvention

Satellite pirates violate the DMCA's umbrella prohibition on circumventing encryption that controls access to a work protected by copyright law.[295] Two of the four classifications of pirates violate this provision "willfully and for the purpose of commercial advantage or private financial gain."[296] The hackers are liable since they willfully research and develop ways to crack the encryption.[297] The card cleaners are liable because they willfully update and apply codes to the access cards to de-scramble the encryption.[298] It is clear that the hackers and the card cleaners are motivated, at least in part, for the purpose of their own financial gain.[299] It is equally clear that they realize that the activity that they are engaging in is illegal.[300]

Since the role of the wholesaler is to market and sell tools that perfect circumvention and not to actually circumvent any encryption, *this provision most likely does not apply to them.*[301] End users seem to be outside the scope of this provision of section 1201 of the DMCA for the reasons set out in Part III.C.1.c of this Article.

b. Creating & Trafficking

Satellite pirates also violate the second provision enumerated in section 1201 of the DMCA.[302] This provision prohibits the creation, marketing, and trafficking of circumvention tools that "(A) is primarily designed or produced for the purpose of circumventing

---

291 *Id.* at (a)(1).
292 *Id.* at (a)(2).
293 *See* SCOTT, *supra* note 10, at 287.
294 17 U.S.C. § 1204(c).
295 17 U.S.C. § 1201(a)(1)(A) (2001) ("No person shall circumvent a technological measure that effectively controls access to a work protected under this title.").
296 17 U.S.C. § 1204(a).
297 *See supra* note 163 and accompanying text.
298 *See supra* notes 179–80 and accompanying text.
299 *See supra* Parts II.E.1.a, II.E.1.c.
300 *See supra* Parts II.E.1.a, II.E.1.c.
301 *See supra* notes 165–71 and accompanying text. It is important to note that it is very likely that these individuals are circumventing encryption to test their products and to pirate signals for their own use. However, this analysis is an exercise meant to isolate the roles of the pirates to better understand their specific liability.
302 17 U.S.C. § 1201(a)(2).

a technological measure . . . ; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure . . . ; or (C) is marketed for use in circumventing a technological measure . . . ."[303] Again, to be criminally liable under this section the pirate must act "willfully and for the purpose of commercial advantage or private financial gain."[304]

Once more, it seems clear that the hackers are criminally liable under this provision since they create, or help to create, the tools used to circumvent encryption.[305] Hackers provide the information that makes the circumvention tools work.[306] The liability of the wholesalers is even more obvious since they are the pirates that sell the circumvention tools and provide forums that post the codes used to de-scramble the satellite signals.[307] The card cleaner's liability stems from the services they provide to the end user — they are middle men — they often purchase and then deliver the circumvention devices to the end users.[308] Additionally, when they update the end users access card they are delivering circumvention devices.[309] It is apparent that the hackers, wholesalers, and the card cleaners are motivated, at least in part, for the purpose of their own financial gain.[310] This provision of the DMCA does not apply to the criminal activity in which end users engage.[311]

E. *Old Theories for a New Crime — Mail & Wire Fraud*

1. The Utility of Mail & Wire Fraud

It may seem strange to discuss such old and general laws in the context of such a cutting edge niche crime; however, those versed in the vernacular of white collar crimes understand the value of these often used laws. Judge Rakoff has noted the importance of mail fraud:

> [t]o federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt 45, our Louisville Slugger, our Cuisinart—our true love. We may flirt with RICO, show off with 10b–5, and call the conspiracy law "darling," but we always

303 *Id.*
304 17 U.S.C. § 1204(a).
305 *See infra* Part II.E.a.
306 *See infra* Part II.E.a.
307 *See supra* notes 165–71 and accompanying text.
308 Interview with Mr. Y, *supra* note 173; *see supra* note 179–80 and accompanying text.
309 Interview with Mr. Y, *supra* note 173 (commenting that he often uses FedEx to mail updated cards to his customers).
310 *See supra* Part II.E.1.a–c.
311 *See supra* Part II.E.1.d.

> come home to the virtues of 18 U.S.C. § 1841, with its simplicity, adaptability, and comfortable familiarity. It understands us and, like so many a foolish spouse, we think we understand it.[312]

A convenient aspect of mail[313] and wire[314] fraud, and a further explanation for their frequent use, is that they are inchoate offenses.[315] Thus, the crime does not have to be perfected and there does not have to be a loss or injury for the laws to apply.[316] Moreover, the offenses are banal — the use of mail or wires to extend a criminal action involving fraud — and easy to prove.[317] Furthermore, these laws are very flexible and are read broadly.[318] They also have sizable penalties, including a maximum fine of $250,000 for individual offenders and $500,000 for organizations and/or up to five years imprisonment.[319] Particularly important to this discussion is that these laws do not require a showing that the defendant personally profited from the scheme to defraud.[320] Additionally, they have been applied to intellectual property law cases since the dawn of the Information Age and they trigger other forms of liability.[321]

2. The Elements & *Mens Rea* of Mail & Wire Fraud

In reviewing these statutes it is clear that they identically treat the fraudulent conduct that they are designed to criminalize.[322] They also have similar elements that must be proven.[323] In order to prove a case of mail fraud, the government must show "(1) a scheme to defraud, and (2) the mailing of a letter, ect. [sic], for the purpose of executing the scheme."[324] In order to prove a case of wire fraud, the government must prove "(1) a scheme to de-

---

312 O'SULLIVAN, *supra* note 12, at 304 (quoting Hon. Jed Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771 (1980)).

313 *See* 18 U.S.C. § 1341 (2001).

314 *See* 18 U.S.C. § 1343 (2001).

315 *See* O'SULLIVAN, *supra* note 12, at 304.

316 *See id.*

317 *See id.*; SCOTT, *supra* note 10, at 394.

318 *See* O'SULLIVAN, *supra* note 12, at 304; SCOTT, *supra* note 10, at 393.

319 18 U.S.C. §§ 1341, 1343.

320 *See* United States v. Silvano, 812 F.2d 754, 759–60 (1st Cir. 1987); *see also supra* note 316 and accompanying text.

321 *See* SCOTT, *supra* note 10, at 393 (citing United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978)). For example, a mail or wire fraud conviction opens the door to the defendant's liability under crimes like RICO and money laundering.

322 *See id.* at 395–96 and nn.19–20.

323 *See id.* at 396.

324 O'SULLIVAN, *supra* note 12, at 304 (quoting Pereira v. United States, 347 U.S. 1, 8 (1954)); *see* United States v. Silvano, 812 F.2d at 759–760 (The mail and wire fraud statutes do not require a showing that defendant sought to personally profit from the scheme to defraud).

fraud, and (2) the use of interstate wire communications in furtherance of the scheme."[325] The case law dictates that the requisite *mens rea* for these crimes is the specific intent to defraud.[326] Furthermore, the mailings must be closely related to the scheme to defraud.[327] For the purpose of these laws, a "mailing" includes any mail delivered by the United States Postal Service or any private or commercial interstate carrier.[328] It is also important that courts and legislatures have broadly interpreted what constitutes a scheme to defraud to include embezzlement, misappropriation of confidential business information, and "depriving the public of the honest services of public officials."[329]

3. Mail & Wire Fraud Can Be Useful in Satellite Piracy Cases

The broad scope of these laws is applicable to satellite television piracy for many reasons,[330] the most important of which are the ambiguities, complexities, and overall inadequacies of the previously analyzed laws and their inability to foil the schemes of the satellite pirates, and specifically the crimes of the end users. Furthermore, these laws are applicable to satellite pirates, because they govern a chief means by which the pirates further their crime.[331]

For example, the wholesalers constantly use the mail to ship their circumvention tools to various purchasers, including card cleaners.[332] End users mail their access cards to the cleaner when its programming requires updating.[333] Accordingly, the card cleaner uses the mail to ship the re-programmed card to the end user.[334] As previously noted, wire-based media, such as computers and the Internet, are the key tools used in satellite piracy.[335] Hackers use these tools in every aspect of furthering their crime.[336] The wholesalers use the Internet to sell their illegal products.[337] The card cleaners download update codes from the Internet, and end

325 SCOTT, *supra* note 10, at 396.
326 *See id.*
327 *See id.*
328 *Id.* at 315 n.9. This law was amended in 1994 to include the private carrier services. *See* 18 U.S.C. § 1341.
329 SCOTT, *supra* note 10, at 397.
330 "The wire fraud statute was enacted to cure a jurisdictional defect that Congress perceived was created by the growth of radio and television as commercial media." *LaMacchia*, 871 F. Supp. at 540.
331 *See, e.g.*, DSS Products, *supra* note 145; Interview with Mr. Y, *supra* note 173.
332 *See, e.g.*, DSS Products, *supra* note 145.
333 Interview with Mr. Y, *supra* note 173.
334 *Id.*
335 *See supra* note 145 and accompanying text.
336 *See supra* note 163 and accompanying text.
337 *See, e.g.*, DSS Products, *supra* note 145.

users may have purchased their pirated access card, which is the foundation of the actual piracy, on the Internet.[338]

4. Applying Mail & Wire Fraud to Intellectual Property Infringement

The issue of whether satellite piracy constitutes a violation of the mail/wire fraud act is quite complex.[339] Despite the conflicting case law, the Computer Crime and Intellectual Property Section of the United States Department of Justice ("CCIPS DOJ") recommends the use of both the mail and wire fraud laws when prosecuting satellite pirates.[340] This Part will briefly examine this complexity and the basis for the CCIPS DOJ's recommendation by analyzing the relevant case law as well as the areas of disagreement between the courts. In doing this, it will focus on two issues. First, it will consider whether intellectual property is covered by the mail and wire fraud laws. Second, it will address the issue of whether an infringement alone is enough to satisfy the fraud requirement to support a mail or wire fraud claim. It will also discuss cases that have been successful in prosecuting satellite pirates under the mail and wire fraud acts with these two considerations in mind.

a. *United States v. McNally*

The case of *United States v. McNally*[341] involved the mail fraud prosecution of a public official of the Commonwealth of Kentucky and a private individual.[342] The defendants were charged with mail fraud under the theory that they "participat[ed] in a self-dealing patronage scheme defraud[ing] the citizens and government of Kentucky of certain 'intangible rights,' such as the right to have the Commonwealth's affairs conducted honestly."[343] The Supreme Court rejected the government's argument that the mail fraud statute in effect at the time was so broad.[344] The Court also noted that the legislative history of the mail fraud statute revealed that the

---

338 Interview with Mr. Y, *supra* note 173.

339 *See* SCOTT, *supra* note 10, at 407–11. *Compare Dowling*, 473 U.S. at 207, *with LaMacchia*, 871 F. Supp. at 539, *and Manzer*, 69 F.3d at 226–28 (holding that the sale of circumvention tools that permitted the pirating of premium satellite broadcasts violates federal fraud statutes).

340 *See Computer Crime*, at ¶ V.B.1.

341 483 U.S. 350 (1987).

342 *See id.* at 352.

343 *Id.*

344 *See id.* at 356 ("The mail fraud statute clearly protects property rights, but does not refer to the intangible right of the citizenry to good government."); *see also Computer Crime*, at ¶ V.B.1 (noting that "[i]n response to the *McNally* decision, Congress enacted 18 U.S.C. § 1346 broadening the definition of a 'scheme or artifice to defraud' to include 'a scheme or artifice to deprive another of the intangible right of honest services.'").

original motivation of the statute was to shield individuals from schemes designed to strip them of their money or property.[345] Moreover, the Court interpreted the statute as being "limited in scope to the protection of property rights."[346] The CCIPS DOJ has noted that if read expansively, *McNally* might be interpreted to preclude all prosecutions for schemes to defraud individuals of intangible property such as intellectual property.[347]

b. *Carpenter v. United States*

In 1987, the same year *McNally* was decided, the Supreme Court also decided *Carpenter v. United States*.[348] The principle defendant in *Carpenter* was employed as a reporter for the Wall Street Journal and wrote a column that discussed information concerning stocks and provided commentary on the paper's assessment of the stock's worth.[349] Due to the perceived quality of the column, the trial court decided that it had the potential to alter the value of the stocks that it scrutinized.[350] Accordingly, the Journal had a policy to keep the contents of the column confidential prior to press time.[351] Nevertheless, the defendant entered into a scheme with members of a brokerage firm to provide advance information concerning the contents of the column.[352] This allowed the conspirators "to buy or sell based on the probable impact of the column on the market."[353]

In arguing that their activities were not a scheme to defraud the *Journal*, within the meaning of the mail and wire fraud statutes, the defendants cited *McNally*.[354] The Court disagreed with the defendants' contention by distinguishing the facts, specifically the fraud, involved in *McNally*.[355] Writing for the Court, Justice White reasoned that confidential business information had "long been recognized as property."[356] He also noted that a scheme to defraud the owner of intangible property, in this case confidential information, was within the scope of the mail and wire fraud stat-

345 *McNally*, 483 U.S. at 356.
346 *Id.* at 360.
347 *See Computer Crime*, at ¶ V.B.1.
348 484 U.S. 19 (1987).
349 *See id.* at 22.
350 *See id.*
351 *See id.* at 23.
352 *See id.*
353 *Id.* (noting that the profits from the scheme were $690,000).
354 *See Carpenter*, 484 U.S. at 25.
355 *See id.*
356 *Id.* at 26.

utes.[357] Accordingly, Justice White noted that,

> "[t]he Journal, as [defendant's] employer, was defrauded of much more than its contractual right to his honest and faithful service, an interest too ethereal in itself to fall within the protection of the mail fraud statute, which had its origin in the desire to protect individual property rights. Here, the object of the scheme was to take the Journal's confidential business information—the publication schedule and contents of the . . . column—*and its intangible nature does not make it any less 'property' protected by the mail and wire fraud statutes.*"[358]

The CCIPS DOJ's analysis echoes *Carpenter's* reasoning by arguing that since intellectual property has been no less recognized as property than as confidential business information, it should be equally protected under the wire and mail fraud statutes.[359] This logic seems difficult to rebut in light of the fact that intellectual property rights are protected by the text of our Constitution[360] and that the Information Age is logically dependent on often intangible pieces of intellectual property. In spite of these considerations, and the rather direct language of the *Carpenter* holding, courts still disagree over the subject.

c. *United States v. LaMacchia*

The prime example of this disagreement, *United States v. LaMacchia*,[361] was briefly discussed in Part III.A in relation to the NET Act. *LaMacchia* is the controversial case in which the titled defendant, a twenty-one year old student at the Massachusetts Institute of Technology ("MIT"), successfully appealed his conviction under the wire fraud act.[362] The defendant was indicted for conspiring with "persons unknown" (end users) to violate the wire fraud statute.[363] The government alleged that the defendant for-

---

357 *See id.*

358 *Id.* at 25 (quoting *McNally*, 483 U.S. at 359 n.8) (emphasis added) (citations omitted).

359 *See Computer Crime*, at ¶ V.B.1. *But see LaMacchia*, 871 F. Supp. at 543 ("As *Dowling* . . . recognized, the copyright holder owns only a bundle of intangible rights which can be infringed, but not stolen or converted. The owner of confidential, proprietary business information, in contrast, possesses something which has clearly been recognized as an item of property") (quoting United States v. Riggs, 739 F. Supp. 414, 422–23 (N.D. Ill. 1990)). *See infra* notes 376–95 and accompanying text for a review and analysis of the Court's holding in *Dowling*.

360 *See* U.S. CONST. art. I, § 8, cl. 8. *But see Dowling*, 473 U.S. at 216, 219 (drawing a distinction between intellectual property (copyright) and tangible property (e.g., automobiles)).

361 871 F. Supp. 535 (D. Mass. 1994).

362 *See id.* at 536.

363 *Id.*

mulated "a scheme to defraud that had as its object the facilitation 'on an international scale' of the 'illegal copying and distribution of copyrighted software' without payment of licensing fees and royalties to software manufacturers and vendors."[364] The defendant used pseudonyms and an encrypted e-mail address to perfect his crime; however, they were not alleged to be or analyzed as part of a scheme to defraud.[365] Further, the government claimed that the scheme resulted in losses that exceeded one million dollars to the copyright holders of the pirated software.[366] A crucial element of the case and, of course, the root of the most obvious controversy surrounding it, is that the government could not allege that the defendant gained or even desired an economic benefit from his infringement.[367]

The even more vexing element of the decision is the court's interpretation of the relevant issue of the case. The court stated that "[t]he issue . . . is whether the 'bundle of rights' conferred by copyright is *unique and distinguishable* from the indisputably broad range of property interests protected by the mail and wire fraud statutes."[368] Even though this issue seems to have been disposed of by *Carpenter*,[369] the court neglected the precise question raised in the case: whether copyright infringement alone is enough to satisfy the fraud requirement of a mail or wire fraud claim.[370] While at first glance these issues may seem identical, they address very different inquiries. As noted, the former focuses on a seemingly settled controversy concerning what type of property is covered by the mail and wire fraud acts.[371] The latter is a more evolved question that seeks to determine if copyright infringement is analogous to a crime based on a more traditional fraud, and if so, whether it

---

364 *Id.* The defendant urged his online acquaintances to upload Excel 5.0, WordPerfect 6.0, and computer games. *Id.* He then directed them to a second encrypted address where the programs were downloaded and accessed with a password. *Id.* The Court noted that "[a]lthough *LaMacchia* was at pains to impress the need for circumspection on the part of his subscribers, the worldwide traffic generated by the offer of free software attracted the notice of university and federal authorities." *Id.* at 536. *Compare LaMacchia*, 871 F. Supp. at 535, *with Manzer*, 69 F.3d at 226. It is also important to note that in *LaMacchia*, the government did not allege a specific misrepresentation or fraud in the indictment. *LaMacchia*, 871 F. Supp. at 537.

365 *Compare LaMacchia*, 871 F. Supp. at 536, *with Manzer*, 69 F.3d at 227.

366 *See LaMacchia*, 871 F.Supp. at 537.

367 *See supra* notes 219, 231–37 and accompanying text (discussing Congress's reaction to *LaMacchia* resulted in the NET Act).

368 *LaMacchia*, 871 F. Supp. at 543 (emphasis added).

369 *See supra* notes 357–58 and accompanying text.

370 *See supra* notes 364–65 and accompanying text (discussing the fact that the court did not mention any other fraud in the indictment). This left infringement as the basis for the wire fraud conviction.

371 *See Carpenter*, 484 U.S. at 26.

would be fair to use it to support a case of mail or wire fraud. Further, the language of the acts does not require an inquiry such as the court's; in fact, neither law prohibits or even mentions a "unique and distinguishable" set of property rights from being within its reach.[372]

Deciding the case under this imprecise premise, the court agreed with the defendant that the government's reliance on the wire fraud statute as a copyright enforcement tool violated the Court's 1985 decision in *Dowling v. United States*.[373] The court also reprinted the antiquated logic concerning intellectual property issues set out in the *Dowling* opinion.[374] In finding for the defendant, the *LaMacchia* court adopted the view that *Dowling* stands for the proposition "that while the holder of a copyright possesses certain property rights which are protectible and enforceable under copyright law, he does not own the type of possessory interest in an item of property which may be 'stolen, converted or taken by fraud.'"[375] *Dowling*'s holding, however, is more limited than this interpretation.

d. *Dowling v. United States*

Dowling involved the extensive bootlegging[376] of Elvis Presley recordings.[377] Although the indictment alleged multiple theories, including mail fraud,[378] the Court only reviewed the allegation that the defendants violated the National Stolen Property Act ("NSPA").[379] The NSPA creates criminal liability for the transpor-

---

372 *See* 18 U.S.C. § 1341 (2001); 18 U.S.C. § 1343; *see also supra* notes 316, 318 and accompanying text.

373 473 U.S. 207 (1985); *see LaMacchia*, 871 F. Supp. at 536 (noting the government contended that *Dowling* only held that copyright infringement does not satisfy the physical taking requirement of the National Stolen Property Act, 18 U.S.C. § 2314).

374 *See LaMacchia*, 871 F. Supp. at 537 ("A copyright . . . is unlike an ordinary chattel because the holder does not acquire exclusive dominion over the thing owned."). "The copyright owner . . . holds no ordinary chattel. A copyright, like other intellectual property, comprises a series of carefully defined and carefully delimited interests to which the law affords correspondingly exact protections." *Id.* (quoting *Dowling*, 473 U.S. at 216).

375 United States v. Riggs, 739 F. Supp. 414, 422–23 (quoting *Dowling*, 473 U.S. at 216–18). The court in *LaMacchia* cites *Riggs* and adopts its reasoning. *See, e.g.*, *LaMacchia*, 871 F. Supp. at 543.

376 *See Dowling*, 473 U.S. at 211 ("A 'bootleg'. . .contains an unauthorized copy of a commercially unreleased performance." The Court also made an important distinction, "[t]hough the terms frequently are used interchangeably, a 'bootleg' record is not the same as a 'pirated' one, the latter being an unauthorized copy of a performance already commercially released." This disparity seems to be based on the immediacy of the commercial value of the property).

377 *See id.* at 211 (stating that the defendants were not authorized to make the copies and that they did not pay royalties to the owners of the copyrighted recordings).

378 *See id.* at 209 (noting that the defendant used the mail to distribute the bootlegged recordings).

379 18 U.S.C. § 2314; *see Dowling*, 473 U.S. at 211.

tation in interstate commerce of "goods, wares, merchandises, securities, or money" that are "stolen, converted or taken by fraud."[380] Therefore, the Court focused on whether the NSPA applied to the interstate shipment of bootlegged and pirated recordings and films whose illicit distribution infringed copyrights — mail and wire fraud were not an issue.[381]

The defendant did not deny that he sold the Elvis bootlegs.[382] In the alternative, he argued that the recordings were not "stolen, converted or taken by fraud."[383] The government admitted, of course, that the actual recordings (the physical records) shipped by the defendant were not wrongfully obtained.[384] Moreover, the government did not allege that the bootlegged copies were identical to the copyrights in Elvis's original recordings, which the defendant infringed by distributing the original performances of those songs.[385] Instead, the government's argument was based on the theory that the bootlegs were within the scope of the NSPA because they "physically embodied performances of musical compositions that [the defendant] had no legal right to distribute . . . [and that] the unauthorized use of the musical compositions rendered the phonorecords 'stolen, converted or taken by fraud' within the meaning of the statute."[386]

In holding that copyrights are not included within the NSPA, the Court noted that the law always applied to tangible "goods, wares, [or] merchandise" that have been "stolen, converted or taken by fraud" and that the statutory language supports the conclusion that a physical taking of property was required.[387] More important to the *LaMacchia* holding, and to this Article, is the Court's diatribe concerning copyright law. The Court commenced this analysis by noting that "[t]he copyright owner . . . holds no ordinary chattel" because they do not have complete control over

---

380 18 U.S.C. § 2314.

381 *See Dowling*, 473 U.S. at 213.

382 *See id.* at 214.

383 *Id.*

384 *See id.* The defendant created the products he sold, he did not steal the physical audio tapes; however, he did steal the content on the records — the heart of the illicit product.

385 *See id.*

386 *Dowling*, 473 U.S. at 214–15.

387 *Id.* at 216, 219 (noting that Congress enacted the NSPA to supplement the National Motor Vehicle Theft Act ("NMVTA"), which was enacted in 1919). The NMVTA was an attempt to supplement the efforts of the States to fight automobile thefts. *See id.* at 219. In other words, the NSPA was specifically designed to fill a particular gap in state law with a federal provision. *See id.* Here, it is important to note that when comparing the mail and wire fraud acts to the NSPA there is no similar limiting factor. In fact, the mail and wire fraud acts were designed to be broad.

all uses of the protected work.[388] The Court cited fair use as an example of when the copyright owners control over the work is limited.[389] This led the Court to the conclusion that "the property rights of a copyright holder have a character distinct from the possessory interest of the owner of simple 'goods, wares, [or] merchandise,' for the copyright holder's dominion is subjected to precisely defined limits."[390] The Court further noted that intrusion of a copyright does not simply equate with a theft, a conversion, or a fraud.[391] Accordingly, the Court also made a distinction between those who infringe a copyright and those who steal an ordinary chattel:

> The infringer invades a statutorily defined province guaranteed to the copyright holder alone. But he does not assume physical control over the copyright; nor does he wholly deprive its owner of its use. While one may colloquially link infringement with some general notion of wrongful appropriation, infringement plainly implicates a more complex set of property interests than does run-of-the-mill theft, conversion, or fraud. As a result, it fits but awkwardly with the language Congress chose—'stolen, converted or taken by fraud'—to describe the sorts of goods whose interstate shipment [NSPA] makes criminal.[392]

Under this rationale, the Court refused to include copyrights in its interpretation of the NSPA.[393] The Court also justified its holding by noting that Congress has "unquestioned" legislative authority over copyrights, and Congress had no reason to include copyrights in a law like the NSPA, which was designed solely to supplement state law.[394] Moreover, the Court noted that when Congress has passed laws criminalizing copyright infringement, it has acted with "exceeding" caution.[395]

e. Justice Powell's Dissent in *Dowling v. United States*

Justice Powell filed a sharp dissenting opinion, which Justice White and Chief Justice Burger joined.[396] He criticized the Court for not explaining how the differences it identified between the

---

388 *Id.* at 216–17. Perhaps, this fact should result in the allotment of greater protection due to the copyright holders vulnerability.
389 *See id.* at 217.
390 *Id.*
391 *See id.*
392 *Dowling*, 473 U.S. at 217–18.
393 *See id.* at 218.
394 *See id.* at 220–21.
395 *Id.* at 221.
396 *See id.* at 229 (Powell, J., dissenting).

rights of a copyright holder and the rights of owners of tangible forms of property are relevant to the language or purpose of the NSPA.[397] In doing so, he noted that the Court was correct in stating that a copyright is "'[comprised] . . . . of carefully defined and carefully delimited interests,' and that the copyright owner does not enjoy 'complete control over all possible uses of his work.'"[398] He went on to argue, however, that while the interference with copyrights may be different from the physical removal of tangible objects, it is not obvious why the difference is material under the NSPA:[399]

> The statute makes no distinction between tangible and intangible property. The basic goal of the National Stolen Property Act, thwarting the interstate transportation of misappropriated goods, is not served by the judicial imposition of this distinction. Although the rights of copyright owners in their property may be more limited than those of owners of other kinds of property, they are surely "just as deserving of protection . . . ."[400]

Furthermore, Justice Powell acknowledged that when Congress passed the Piracy and Counterfeiting Amendments Act of 1982,[401] it provided that the new penalties "shall be in addition to any other provisions of Title 17 *or any other law*."[402] Additionally, he argued that the defendants "'could not have doubted the criminal nature of their conduct. . . .' [Their] claim that [the NSPA] does not reach his clearly unlawful use of copyrighted performances evinces 'the sort of sterile formality' properly rejected by the vast majority of courts that have considered the question."[403]

f. The Weight of *Dowling v. United States* in a Digital Environment

Today, the problems with the *Dowling* Court's treatment of copyrighted material have become magnified. In fact, the Court's contention regarding Congress's unwillingness to radically expand

---

397 *See id.* at 230.

398 *Dowling*, 473 U.S. at 230 (quoting Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 432 (1984)) (citations omitted).

399 *See id.*

400 *Id.* at 230–31 (quoting United States v. Drum, 733 F.2d 1503, 1506 (1984)). Here, it is important to note that the mail and wire fraud statutes do not make a distinction between tangible or intangible property.

401 Pub. L. 97-180, 96 Stat. 91.

402 *Dowling*, 473 U.S. at 233 (Powell, J., dissenting) (quoting 18 U.S.C. § 2319(a)) (alteration in original).

403 *Id.* (quoting United States v. Bottone, 365 F.2d 389, 394 (1966), cert. denied, 385 U.S. 974 (1966) and United States v. Belmont, 715 F.2d 459, 462 (1983), cert. denied, 465 U.S. 1022 (1984)) (citations omitted).

criminal copyright law no longer holds water.[404] When the Information Age became digitalized and the Internet popularized, Congress became less interested in being careful not to push criminal copyright too far.[405] The primary reason for this is that in a digital environment, a pirate can make perfect copies of a protected work that can be duplicated and reduplicated without the quality of the copies being compromised.[406] Evidence of Congress's fierce reaction to this activity is the passage of the NET Act, the DMCA and to a lesser extent, the Copyright Term Extension Act ("CTEA").[407] Therefore, in 1985, when *Dowling* was decided, it may have made sense to formulate a distinction between copyrighted property and tangible property based upon Congressional treatment of them with respect to the criminal law; however, it no longer makes sense today.[408] Of course, the central premise of *Dowling* was, and still is, flawed.[409] Although an infringer does not wholly divest a copyright holder of the use of the protected work,[410] he does deprive the copyright holder of something equally as important — the monetary value of the stolen copyrighted work, or in other words, the market share that is seized by the pirate. Certainly, the promotion of science and the useful arts that the Copyright Clause seeks to champion is hollow without a viable means of enforcing it on a criminal level.

g. *LaMacchia*'s Reliance on *Dowling v. United States*

Nevertheless, the *LaMacchia* court adopted the backward views on intellectual property that the *Dowling* Court professed and extended its holding over a case that involved a very different law.[411] Consequently, even if the *LaMacchia* court found the Court's reasoning persuasive, it was not a relevant enough basis upon which to

---

404 *See supra* note 395 and accompanying text.

405 *See* Lampman, *supra* note 219, at 386 n.192, 387–99 (discussing the DMCA); *see supra* notes 231–37 and accompanying text (discussing the dramatic change created by the NET Act).

406 *See* Lampman, *supra* note 219, at 383.

407 *See id.* at 370–72. Although these laws were passed a year after *LaMacchia* was decided — with the exception of the NET Act, which was passed immediately after *LaMacchia* and in direct response to it — they were contemplated in the years leading up to the *LaMacchia* case. *See, e.g.*, Lampman, *supra* note 219, at 386–90. Moreover, the dilemmas the laws attempted to address were no secret to the general legal community, and should have been apparent to the *LaMacchia* court.

408 *See* ROBERT G. MCCLOSKEY, THE AMERICAN SUPREME COURT 233 (3d ed. 2000) ("The Court must alter its own perspectives as history's perspectives are altered, yet must not move so fast that the idea of continuity is lost.").

409 *See Dowling*, 473 U.S. at 217–18 (1985).

410 *See id.*; *see also supra* notes 388, 390–92 and accompanying text.

411 *See supra* note 379–81 and accompanying text.

found their entire opinion.[412] *Dowling* clearly considered and was influenced by the legislative purpose of the NSPA.[413] As noted, the NSPA does not share a similar intent or history with the mail or wire fraud act. Perhaps the only similarity these criminal laws have is that neither of them distinguishes between tangible and intangible property.

Beyond this flaw, the *LaMacchia* court also misinterpreted the mail and wire fraud laws in holding that they were narrowly drafted. For example, in an obtuse response to the government's argument, the court stated:

> The suggestion that the felony provisions of the wire fraud statute were enacted with the punishment of copyright infringement in mind is somewhat difficult to accept when one remembers that in 1952 the Copyright Act authorized only misdemeanor prosecutions, a circumstance that continued until 1982. Equally difficult to accept is the idea that Congress has in some fashion acquiesced by silence to the utilization of mail and wire fraud as copyright enforcement tools.[414]

In his stirring dissenting opinion in *McNally*,[415] which was written ten years prior to *LaMacchia*, Justice Stevens refuted a similar argument and expressed important issues concerning the mail and wire fraud statutes.[416]

h. Justice Stevens's Dissent in *United States v. McNally*

Justice Stevens commenced his discussion by conducting an originalist examination of the mail fraud statute, focusing on the meaning of the term "fraud."[417] He noted that in 1872, when the statute was first enacted, fraud had a broad commonly understood meaning.[418] He provides three definitions of "fraud" that were contemporary to the first mail fraud law as examples of the term's expansive meaning.[419] He first stated that Justice Story's 1870 manuscript cited the definition of "fraud" as "appl[ying] to every artifice made use of by one person for the purpose of deceiving

---

412 *See LaMacchia*, 871 F. Supp. at 541.

413 *See Dowling*, 473 U.S. at 220–21; *see also supra* notes 379, 387 and accompanying text.

414 *LaMacchia*, 871 F. Supp. at 543 n.13.

415 483 U.S. 350, 362, 377 (1987) (Stevens, J., dissenting); *see supra* note 344 and accompanying text (noting that Congress responded to *McNally* by passing 18 U.S.C. § 1346).

416 *See id.* at 373.

417 *Id.* at 368–73; *see, e.g.*, Antonin Scalia, *Originalism: The Lesser Evil*, 57 U. CIN. L. REV. 849, 864 (1989); *see supra* note 322 and accompanying text (noting that the wire fraud act is nearly identical to the mail fraud act); *see also Carpenter*, 484 U.S. at 25 n.6.

418 *See McNally*, 483 U.S. at 370.

419 *Id.* at 370–71.

another," or as "any cunning, deception, or artifice used to circumvent cheat, or deceive another."[420] He then turned to the popular law dictionaries of the period to determine what conduct constituted "defrauding" an individual.[421] The first of which explained that "*[t]o defraud is to withhold from another that which is justly due to him,* or to deprive him of a right by deception or artifice."[422] The second law dictionary interpreted "defraud" as "*to cheat*; to deceive; to deprive of a right by an act of fraud . . . *[t]o withhold from another what is justly due him,* or to deprive him of a right, by deception or artifice."[423]

Justice Stevens compared the mail and wire fraud statutes to the Sherman Act and the civil rights legislation that were drafted in expansive language, so that courts would have a broad range in interpreting them and the remedial purposes that Congress identified would be achieved.[424] He characterized this sort of legislation as the legislature delegating its authority to the courts, which would have the duty of filling the gaps.[425] He then directly addressed the type of mistake that the *LaMacchia* court made by suggesting that the meaning of the wire fraud law was fixed in 1952.[426] One court has noted, "[t]he notion that the meaning of the words 'any scheme or artifice to defraud' was frozen by a *special conception* of the term recognized by Congress in 1872 is manifestly untenable."[427] Justice Stevens then quoted Judge Posner, who further criticized *LaMacchia*'s line of reasoning:

> The argument depends on the view that the meaning of fraud in the mail-fraud statute was frozen by the conception of fraud held by the framers of the statute when it was first passed back in the nineteenth century. This seems to us the opposite and equally untenable extreme from arguing that fraud is whatever strikes a judge as bad, but in any event the 'intangible rights' concept that the argument attacks is too well established in the courts of appeals for us to disturb.[428]

Additionally, Justice Stevens argued that legislative history does not suggest that the mail fraud statute intended for "fraud" to

---

420 *Id.* at 370 (quoting 1 JOSEPH STORY, EQUITY JURISPRUDENCE § 186 (11th ed. 1870)).
421 *Id.*
422 *Id.* (quoting 1 JOHN BOUVIER, BOUVIER'S LAW DICTIONARY 530 (Boston Book Co. 1897)) (emphasis added).
423 *Id.* at 370–71 (quoting WILLIAM ANDERSON, A DICTIONARY OF LAW 474 (1996)) (emphasis added).
424 *See McNally*, 483 U.S. at 372–73.
425 *See id.* at 373.
426 *See id.*; *supra* note 414 and accompanying text.
427 *McNally*, 483 U.S. at 373 (emphasis added).
428 *Id.* (quoting United States v. Holzer, 816 F.2d 304, 310 (1987)).

have a more restricted meaning than the commonly understood meaning.[429] Moreover, he acknowledged that the general nature of the mail fraud law has often been interpreted to cover novel species of fraud and that Congress had amended the statute to support a broad interpretation.[430] Justice Stevens buttressed his argument by quoting Judge Rakoff's influential article:

> First enacted in 1872, the mail fraud statute, together with its lineal descendant, the wire fraud statute, has been characterized as the 'first line of defense' against virtually every new area of fraud to develop in the United States in the past century. Its applications, too numerous to catalog, cover not only the full range of consumer frauds, stock frauds, land frauds, bank frauds, insurance frauds, and commodity stock frauds, but have extended even to such areas as blackmail, *counterfeiting*, election fraud, and bribery. In many of these and other areas, *where legislatures have sometimes been slow to enact specific prohibitory legislation, the mail fraud statute has frequently represented the sole instrument of justice that could be wielded against the ever-innovative practitioners of deceit.* During the past century, both Congress and the Supreme Court have repeatedly placed their stamps of approval on expansive use of the mail fraud statute. Indeed, each of the five legislative revisions of the statute has served to enlarge its coverage.[431]

In light of this argument, the inexcusable flaws at the heart of *LaMacchia*'s holding and the limited applicability of *Dowling*, it seems that what the *LaMacchia* court actually found in *Dowling* was, in practical terms, a basis for the precocious MIT student's salvation.[432] The cases, dissents, and laws discussed here, along with Congress's expansion of criminal copyright in direct response to developments in the Information Age, seem to indicate that if the *LaMacchia* court addressed the correct issue in the case — whether copyright infringement alone is enough to satisfy the fraud requirement of a mail or wire fraud claim — they would have been led to the conclusion that it is.

i. Applying Mail & Wire Fraud Specifically to Satellite Piracy

In making their recommendation in favor of using the mail and wire fraud laws to combat satellite piracy, the CCIPS DOJ re-

---

429 *Id.* (arguing that there is no evidence of Congress ever limiting the scope of the mail fraud statute); *see also supra* notes 418–23 and accompanying text.

430 *See McNally*, 483 U.S. at 373.

431 *Id.* at 374 (quoting Hon. Jed Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771, 772–73 (1980)) (emphasis added).

432 *See supra* note 362 and accompanying text.

lied on a number of cases in which satellite piracy was successfully prosecuted using these theories.[433] In these cases, the courts relied on different concepts in linking fraud to satellite piracy. In doing this, however, it often seems as though the courts are reaching to fit a scheme to defraud into the act of piracy. For instance, in *United States v. Manzer*,[434] the court held that the evidence of the defendant's illicit business practices constituted intent to defraud.[435] The factors that the court weighed in making this determination included, "[t]he type of technology sold, the volume of sales, the nature of his clientele, the level of secrecy employed [the defendant gave a false address and used an alias], and the fact that his operation" manufactured tools to intercept encrypted broadcast signals.[436] When considering the evidence of fraud, and especially the fact that the true fraudulent activity — giving a false address and using an alias — is a diminutive portion of the crime, it seems that the effect of the *Manzer* court's holding is the quiet approval of the prosecution of a defendant whose actual scheme to defraud was mere infringement and that infringement alone is enough to satisfy the fraud requirement to bring a mail or wire fraud claim.[437]

However, a more daring court in *United States v. Coyle*[438] bluntly held that the defendant's infringement of television programming, coupled with his use of the mail, satisfied the requirements of the mail fraud act.[439] The court reasoned that the defendant's activity was a scheme or artifice to defraud within the meaning of the mail fraud statute because it deprived the cable companies of their "property rights by dishonest methods or schemes."[440] The defendant, who sold descrambling devices, argued that the Supreme Court's holding in *Dowling* shielded him

---

433 *See* United States v. Manzer, 69 F.3d 222, 226–28 (8th Cir. 1995); United States v. Coyle, 943 F.2d 424, 427 (4th Cir. 1991) (holding the sale of cable television unscramblers a scheme to defraud "because it wronged the cable companies in their 'property rights by dishonest methods or schemes'") (quoting United States v. McNally, 483 U.S. 350, 358 (1987)); United States v. Norris, 833 F. Supp. 1392, 1394–96 (N.D. Ind. 1993).

434 69 F.3d at 226–28.

435 *Id.* at 227.

436 *Id.*

437 *See id.* at 225 (noting that the claim that the defendant violated 47 U.S.C. § 605(e)(4) was dismissed prior to trial since it did not become effective until January 1, 1989, more than six months after the charged conduct took place).

438 943 F.2d at 424. Although the facts of this case dealt with 47 U.S.C. § 553, which is the law that applies to the piracy of cable television, it is very similar to 47 U.S.C. § 605. When addressing the issue of mail or wire fraud, there is no difference between cable or satellite piracy. *See, e.g.*, Time Warner Cable v. Dockins, No. 96 Civ. 6852, 1998 U.S. Dist. LEXIS 22689, at *9; *see also supra* note 238 and accompanying text.

439 *See Coyle*, 943 F.2d. at 427.

440 *Id.*

from prosecution under the mail fraud statute.[441] In dismissing this argument, the court simply noted that the mail fraud statute is not so restrictive and that "any scheme or artifice to defraud" is to be construed broadly.[442] The court also echoed one of the arguments made by Justice Stevens in his dissent to the *McNally* holding[443] in stating that, "the mail fraud statute does not by its terms define fraud. It generally leaves to other statutes the specifications of what conduct constitutes a scheme to defraud."[444] The court then held that the law designed to protect the revenue of television cable companies from the piracy of their programming is such a statute.[445] Of course, this logic would extend to 47 U.S.C. § 605, the statute that serves to protect satellite providers from piracy.[446]

j. Answering the Questions

Therefore, intellectual property is covered by the mail and wire fraud laws and infringement alone is enough to satisfy the fraud requirement to support a mail or wire fraud claim. The first of these claims is supported by Justice Stevens's dissent in *McNally*, which was swiftly followed by Congress overruling the majority's holding, the Court's holding in *Carpenter*, Justice Powell's logical dissent in *Dowling*, and of course, the plain meaning of the text of the mail and wire fraud laws. The second argument is again supported by Justice Stevens's dissent in *McNally*, the Court's holding in *Carpenter*, Justice Powell's logical dissent in *Dowling*, the plain meaning of the text of the mail and wire fraud laws, and additionally, Congress's recent and swift expansion of criminal copyright law, as well as the holding in *Coyle*, and to a lesser extent, the holding in *Manzer*.

5. The Potential Liability of the Various Satellite Pirates Under Mail & Wire Fraud

Even if a court is not willing to decide that infringement alone is enough to satisfy the statutes, when evaluating the fraudulent aspects of satellite piracy and the relevant case law, it seems likely that hackers, wholesalers, and card cleaners are still within the stat-

441 *See id.* at 426.

442 *Id.* (quoting Durland v. United States, 161 U.S. 306, 313 (1987), which quotes Hammerschmidt v. United States, 265 U.S. 182, 188 (1924)).

443 *See supra* note 418 and accompanying text.

444 *Coyle*, 943 F.2d at 427.

445 *See id.*

446 *See supra* note 238 and accompanying text. *Compare Dowling*, 473 U.S. 207 (1985), *with Coyle*, 943 F.2d at 424. The infringement and overall criminal activity in these cases seems particularly similar, while their treatment of infringement is very different.

utes' scope, as they are currently applied.[447] In other words, the fraudulent elements of their criminal activity often seems substantial enough to fairly prosecute them under these laws.

Finally, there is a law that also seems to apply to end users; however, in the absence of Congressional action, reaching all end users is most likely dependent on two factors. First, courts must adopt the view that infringement alone is enough to satisfy the fraud requirement in the mail and wire fraud statute. This is because the end user's fraudulent activities are usually insignificant and not directly linked to the actual crime.[448] In fact, it appears that most end users do not commit the type of fraud traditionally necessary to trigger these statutes.[449] The uncertainties of how this law will be applied to all classes of satellite pirates may severely hamper the prosecution of this white collar crime. Second, federal prosecutors must be willing to use these laws to prosecute criminals that may appear sympathetic.[450]

IV. THE NEED FOR SPECIFIC LEGISLATION

> "The greatest trick the Devil ever pulled was convincing the world he didn't exist."[451]

The above quote is taken from the film, *The Usual Suspects*.[452] In this film, the protagonist, Verbal, tricks the supporting characters into believing that he is a weak, simple minded individual, when in truth, he is a criminal mastermind.[453] In the process of his masquerade, he sets the other characters up with his crime before telling a fantastic tale in a police station interview.[454] Before the cops turn wise to his lies, he vanishes without a trace.[455]

---

447 *See supra* notes 163–64, 171, 179–80 and accompanying text (noting the fraudulent activities of these pirates).

448 *But see supra* notes 436–37 and accompanying text.

449 *See supra* notes 184–86 and accompanying text (noting the fraudulent activities of the end users); *see also Computer Crime*, at ¶ VI.B.1.b (noting that "in the absence of strong evidence of misrepresentation," a prosecutor may prefer not to proceed with a wire or mail fraud charge if an infringement crime may be charged).

450 *See supra* notes 197–98 (discussing that when apprehended white collar criminals often appeal to prosecutor's sympathies).

451 Christopher McQuarrie, *The Usual Suspects*, ¶ 77, *available at*, http://www.godamongdirectors.com/scripts/usual.shtml (last visited Sept. 1, 2004) (quoting CHARLES PIERRE BAUDELAIRE, PARIS SPLEEN 61 (Louise Varèse trans., New Directions 8 ed. 1970) (1869). In Varèse's translation, the quote reads, "[m]y beloeved brothers, never forget when you here people boast of our progress in enlightenment, that one of the devil's best ruses is to persuade you that he does not exist!").

452 *See id.*

453 *See id.*

454 *See id.*

455 *See id.*

While not the devil, or even criminal masterminds, this quote applies to end users and to a lesser extent, to all satellite pirates. Again, it is estimated that there are as many as three million people in America that would properly fall into the category of an end user of pirated satellite television. Of course, the suspects would be unusual when the crime they commit is invisible.

On the rare occasion that end users are noticed, they are treated as small-time infringers who are not culpable since they do not further the crime.[456] While this may seem to be the case, the fact is that these people constitute the demand for a one billion dollar a year criminal industry. Still, they are ignored by most prosecutors and all of Congress. In fact, the laws rarely speak to their role in this crime, and when they do, it only gives them an incentive to steal.[457]

Similarly, the true white collar criminals involved in satellite piracy, the circumventors (hackers), the investors (wholesalers), and the rogue satellite dealers (card cleaners) have not received the scrutiny that they deserve. The reports of their arrests are few and the topic of their crimes is given little attention by the media. The scholarly legal community pays even less attention to the crime — the last wave of law review articles addressing the crime were published in the early 1980s.

Moreover, of the laws discussed in Part III, there are none that provide the practical framework for a holistic and specific strategy to prosecute the crime of satellite piracy. Further, the multiple theories used to prosecute this crime only foster additional and unnecessary confusion. In fact, each of these laws is flawed in that end users — the players who make satellite piracy profitable — are not directly covered by the law or are only subjected to minimal liability.

Congress must create a specific law that carefully addresses the various issues involved with this crime. The issue of increasing the liability for end users should be high on their agenda. Until people understand that circumventing satellite signals is a crime that carries strict consequences, they will not be deterred from engaging in the crime and the demand for piracy will continue to grow. However, if end users can be deterred, the crime of satellite piracy would lose its profitability.

---

456 *See, e.g.*, Entertainment By J & J, Inc., v. Mario Perez, No. C99-4261TEH, 2000 U.S. Dist. LEXIS 9280, at *11 (N.D.Cal. June 30, 2000) (noting a civil case in which the court was lenient on the more culpable type of end user, the restaurant or shop owner who uses pirated pay-per-view events to attract customers).

457 *See supra* notes 254–56 and accompanying text (discussing 47 U.S.C. § 605(d)(5)).

In the absence of such a law, there is great importance in clarifying the availability of the mail and wire fraud statutes to prosecute this crime. The Court should clearly define the issue of whether intellectual property is within the scope of the mail and wire fraud statute and, if so, if infringement alone is enough to trigger liability. It is within their duty to settle this debate, especially in light of their expansive reading of the statutes in *Carpenter*.[458] If the Court refuses to act, then Congress must. Congress should amend these laws to extend to criminal activity like satellite piracy, since they will effectively apply to each class of pirate, and like in other white collar crimes, provide a basis for prosecution. Congress cannot risk the fate of pretending that these criminals do not exist — the vigor of the Information Age may depend upon their action.

[458] 484 U.S. 19 (1987).

APPENDIX A[459]

DSSHELPER.COM

LEGAL DISCLAIMER

By entering this web site, you hereby and *without exception* agree to the following terms and conditions of use and legal restrictions.;

1) You understand that this website, and all directly associated web sites are wholly owned, operated and hosted in the sovereign province and nation of Alberta, Canada and are operated in accordance to the applicable laws and statutes of Canada and Alberta. We make no representation that the materials on this site are appropriate for use outside Canada.

2) You understand that this web site's intended audience are residents of Canada and other countries where use of test cards is considered legal. You understand that the worldwide nature of the internet makes it impossible to regulate the audience and it is possible to access this web site in countries where use of test cards is illegal. You understand that it is your responsibility to check your local laws before committing any information on this website for any given practical use. We do NOT condone signal theft and you are absolutely prohibited from putting ANY information on this site to any illegal use. Any individuals indicating illegal intent are subject to loss of any and all privileges given to them by this web site.

3) You understand that use, possession, distribution, manufacture or importation of test cards is illegal in the United States. If you are a U.S. resident, you are required by law to subscribe and the use or sale of test cards of any kind is unlawful and constitutes signal theft and is subject to criminal and civil penalties according to U.S. law. We do not condone the use or sale of test cards to U.S. residents. In addition, use of test cards may also be considered illegal in any country or jurisdiction where the U.S. based services of Directv Inc. and Echostar Communications Corp, in specific, The Dish Network can legally and lawfully distribute their signals, either directly or indirectly and make said signals available for purchase to consumers on a subscription basis.

---

459 This is a copy from DssHelper.com, *at* http://www.dsshelper.com/terms.shtml (last visited Sept. 1, 2004). DssHelper.com does not sell circumvention equipment directly on their site; however, they inform potential pirates how to circumvent encryption, they provide a chat room forum for the sharing and updating of the requisite codes for circumvention, and they review the quality of encryption products and provide direct links to sites that do sell the encryption products. *See* HULOADERS.com, *at* http://www.huloaders.com/disclaimer.php (last visited Apr. 18, 2003). The disclaimer for HULOADERS.com is printed in Appendix B.

4) You understand that all information on this web site is informational in nature and is protected by the fundamental right of free speech GUARANTEED by both the United States Constitution and Canadian Charter of Rights and Freedoms. As outlined above, although simple access of the information on this site may be legal and protected under various constitutions and charters, physical use may NOT be legal in certain countries and jurisdictions, in specific, The United States. If you are in doubt, you should seek legal advice BEFORE putting any information on this site to a practical use.

5) You understand that this web site does NOT sell, lease, rent, manufacture, import, export, install or distribute test cards of ANY kind. In addition, we do NOT sell products of ANY kind, either directly or indirectly, nor do we offer any consultation in regards to any of the content contained in this web site. Please do not even ask.

6) You understand that you are solely responsible for your own actions and agree to hold this web site and its principals harmless for any difficulties incur[r]ed through physical use of any of the information contained on this web site.

7) This web site is not aff[i]liated in any way, shape or form, either legally or professionally with Directv Inc. United States Satellite Broadcasting Ltd., Echostar Communications Corp., News Datacom Ltd., News Data Systems Americas or their affiliates, both private, commercial, domestic and international.

8) You agree that this Web Site is privately owned and operated. Employees, Agents or Solicitors both direct and indirect of Directv Inc., News Datacom Ltd, NDS Americas Inc. or Echostar Communications Corporation are STRICTLY prohibited from entering this site and are directed to leave immediately. Failure to comply may constitute a criminal act of trespassing.

9) By entering this site, you agree that the laws of the Province of Alberta, Canada will, without regard to the conflicts of laws or principles of any other foreign nation or jur[isd]iction thereof, apply to any and all matters relating to the use of this web site. Furthermore, you understand that any challenge to this web sites operation or legality MUST be in direct reference to Canadian laws and statutes only and must clearly show with documented evidence that Canadian law prohibits exchange of information in relation to reception of foreign broadcasts that are neither lawfully authorized by the Canadian Radio and Telecommunications Commission (CRTC) nor intended for reception in Canada by their broadcasters. In addition, any challenge must also be accompanied with

documented evidence that specifically and clearly shows that a Canadian Court of law has successfully upheld a ruling that such exchange of information is in fact unlawful on Canadian soil. In absence of such documentation, any challenge to this web site may NOT be legal and may in fact constitute a criminal act of harassment.

10) You agree that neither of the U.S. based services of Directv Inc. nor Echostar Communications Corp. currently hold ANY distribution rights to their signals on Canadian soil, nor are they considered or legally recognized to be LAWFUL distributors of their respected signals in Canada and are NOT authorized or legally sanctioned to conduct broadcasting services, either directly or indirectly of any kind in Canada in relation to their respected broadcasting signals. Furthermore, as the broadcasting services of Directv Inc. and Echostar Communications Corp. cannot legally be distributed within Canada, their broadcasts have been legally interpreted as "foreign signals" and Canadian Law has also been legally interpreted as NOT currently regulating nor protecting "foreign signals." Canadian law has been legally interpreted to regulate and protect signals originating ONLY from a "Lawful" Canadian Distributor. This has been decided and UPHELD in several recent Canadian legal proceedings. Court transcripts of these proceedings are available on request.

11) You agree that this web site contains no information in whole or in part relating to ANY LAWFUL Canadian broadcaster. Currently, the broadcasting services of Star Choice Communications Inc. and Bell Expressvu L.P. whose respected signals are distinctly sovereign in nature and are regulated in full by the Canadian Radio and Telecommunications Commission (C.R.T.C.), are the only LAWFULLY authorized distributors of Direct to Home Services in Canada. Neither Star Choice Communications Inc, nor Bell Expressvu L.P. currently hold ANY distribution or re-broadcast rights to the U.S. Based services of Directv Inc. or Echostar Communications Corp. In addition, it is understood that the current TVRO equipment standard of Directv Inc. or Echostar Communications Corp. is not directly compatible with any LAWFUL Canadian DTH broadcaster. This web site without reservation, recognizes the lawful distributor status of Star Choice Communications Inc. and Bell Expressvu L.P. and offers NO information of any kind relating to either of these distinctly sovereign broadcasting services.

12) You understand that if you do not agree with any of the above conditions, then you are directed to *leave now*!

APPENDIX B[460]

HULOADERS.COM

DISCLAIMER

By viewing this website and/or purchasing any HULOADERS.com devices, you verify that you have read and fully agree to these terms.

HULOADERS.com is not affiliated in any way, shape, or form, legally or professionally, with DirecTv Inc., USSB., or any of their affiliates, private, commercial, or civil (domestic or international).

You understand that HULOADERS.com does not promote nor condone signal theft of any kind and you do not hold HULOADERS.com responsible for the actions of any of their users as it is the users' responsibility to comply with all local and State laws of their territory and country. If you live in an area where you can legally subscribe to satellite broadcasting or if you are a company that uses smart cards for encryption or storing codes it may be ILLEGAL to use the devices from HULOADERS.com.

This site is for educational and informational purposes ONLY. It is not our intention to assist you in committing fraud or performing any illegal acts. As with any action you take, it is your sole responsibility to obey any regulations or laws that apply to you. The presence of this site on the world-wide-web means that it is available to a world audience, so we cannot possibly advise you on the legality of utilizing or possessing the information contained herein. You should always seek competent legal counsel to insure you are in compliance with all local laws.

HULOADERS.com cannot be held responsible for any damage or loss of DSS equipment including but not limited to: Access Card, IRD (Receiver), or any other DSS equipment. By viewing this web page and purchasing any DSS devices, you verify that you have read and fully agree to these terms.

460 This is a copy from HULOADERS.com, *at* http://www.huloaders.com/disclaimer.php (last visited Apr. 18, 2003). HULOADERS.com sells a variety of encryption tools.