

H

United States District Court,
E.D. Texas,
Beaumont Division.

Ethan SHAW, and Clive D. Moon, On Behalf of
Themselves and All Others
Similarly Situated, Plaintiffs,

v.

TOSHIBA AMERICA INFORMATION SYSTEMS,
INC., NEC Electronics, Inc., Toshiba
Corporation, Toshiba America, Inc., and Toshiba
America Electronic, Components,
Inc., Defendants.

No. 1:99-CV-0120(TH).

Aug. 26, 1999.

Purchasers of allegedly defective laptop computers sued manufacturer and software developer under civil suit provision of Computer Fraud and Abuse Act. On defendants' motions for summary judgment, the District Court, Heartfield, J., held that: (1) manufacturer's sale of laptop computers containing floppy-diskette controllers with allegedly defective microcode was "transmission," within meaning of Act; (2) plaintiffs had standing to seek injunctive relief; and (3) software developer could be held liable for violating Act.

Motions denied.

West Headnotes

[1] Statutes  **181(1)**
[361k181\(1\) Most Cited Cases](#)

Court's goal in interpreting language of statute is to give effect to Congress' intent.

[2] Statutes  **188**
[361k188 Most Cited Cases](#)

Absent congressional direction to the contrary, words in statutes are to be construed according to their ordinary, contemporary, common meanings.

[3] Statutes  **184**
[361k184 Most Cited Cases](#)

[3] Statutes  **205**
[361k205 Most Cited Cases](#)

To interpret statutory terms, court examines statute as a whole, including its design, object, and policy.

[4] Statutes  **208**
[361k208 Most Cited Cases](#)

When interpreting statute, court defines particular terms with reference to specific context in which they are used, and looks to arrangement of certain terms within statute as guide to their meaning.

[5] Statutes  **188**
[361k188 Most Cited Cases](#)

Court must depart from plain meaning of statutory text if it would lead to result so bizarre that Congress could not have intended it.

[6] Statutes  **217.4**
[361k217.4 Most Cited Cases](#)

When statutory language is susceptible to more than one reasonable interpretation, court should look beyond statutory text and examine legislative history to divine congressional intent.

[7] Statutes  **216**
[361k216 Most Cited Cases](#)

[7] Statutes  **217.3**
[361k217.3 Most Cited Cases](#)

If court determines that departure from plain meaning of statutory text is warranted, it may look to official committee reports, conference reports, and contemporaneous statements by legislators on committee that drafted statute.

[8] Telecommunications  **461.15**
[372k461.15 Most Cited Cases](#)

Manufacturer's sale of laptop computers containing floppy-diskette controllers with allegedly defective microcode was "transmission," within meaning of Computer Fraud and Abuse Act provision prohibiting transmission of code which intentionally causes damage to protected computers. [18 U.S.C.A. § 1030\(a\)\(5\)\(A\)](#).

[9] Statutes  **241(1)**
[361k241\(1\) Most Cited Cases](#)

Principle of strict construction of criminal statutes does not mean that they must be given their

narrowest possible meaning.

[10] Injunction  **114(2)**
[212k114\(2\) Most Cited Cases](#)

Purchasers of allegedly defective laptop computers had standing to seeking injunction requiring manufacturer to advise all potential purchasers that computers could corrupt and destroy data without warning.

[11] Criminal Law  **26**
[110k26 Most Cited Cases](#)

General principle of causation in criminal law is that individual with necessary intent may be held liable if he is cause in fact of criminal violation, even though result which law condemns is achieved through actions of innocent intermediaries.

[12] Torts  **15**
[379k15 Most Cited Cases](#)

Intervening act, tortious or criminal, will insulate defendant from liability only when defendant could not have reasonably anticipated subsequent act.

[13] Telecommunications  **461.15**
[372k461.15 Most Cited Cases](#)

Designer of allegedly defective microcode used in computer floppy-diskette controllers could be held liable, under Computer Fraud and Abuse Act provision prohibiting transmission of code which intentionally causes damage to protected computers, for third party's sales of computers incorporating controllers which contained defective code; designer could have reasonably anticipated such sales. [18 U.S.C.A. § 1030\(a\)\(5\)\(A\)](#).

*[927 Hubert Oxford, III](#), Benckenstein & Oxford, Beaumont, TX, [Gilbert Irvine Low](#), Orgain Bell & Tucker, Beaumont, TX, [Charles Silver](#), Austin, TX, L. DeWayne Layfield, Beaumont, TX, for Ethan Shaw, Clive D. Moon.

[Walter Joshua Crawford, Jr.](#), Crawford & Olesen LLP, Beaumont, TX, [Reagan Mark Brown](#), [Frank G. Jones](#), [David Jack Levy](#), Fulbright & Jaworski, Houston, TX, for Toshiba American Information Systems Inc., Toshiba Corp., Toshiba America Inc., Toshiba America Electronics Components Inc.

[Walter B. Stuart, IV](#), [Allan VanFleet](#), [Erica L. Krennerich](#), Jason M. Powers, Vinson & Elkins, Houston, TX, [Lawrence Louis Germer](#), Germer &

Gertz, Beaumont, TX, for NEC Electronics Inc.

[Jeffrey L. Simpton](#), Office of Atty. Gen., Sacramento, CA, for State of California.

[Michael Rosenblat](#), Office of Ill. Atty. Gen., Chicago, IL, for State of Illinois.

John Mark Kraus, Asst. Atty. Gen., Dept. of Legal Affairs, Tallahassee, FL, for State of Florida.

Mike Bradford, U.S. Atty., Beaumont, TX, for U.S.

Joseph Charles Blanks, Doucette, TX, for Laura Bates.

[Benjamin E. Baker, Jr.](#), John P. Willis, IV, [M Clay Alspaugh](#), Hogan Smith & Alspaugh, Birmingham, AL, for Biehl & Co., Inc.

Lawrence Smith, Joliet, IL, pro se.

Dawn L. Phillips-Hertz, Troy, MI, pro se.

[Daniel R Castro](#), Watt Castro & Houser, Austin, TX, for Maxtor Corp.

[Charles M. Thompson](#), [Kearney Dee Hutsler](#), Thompson Hutsler Law Firm, Birmingham, AL, for J T Karney, Southern Network Services Inc.

[Mark Allen Lindow](#), Lindow & Treat, San Antonio, TX, for Lindow & Treat LLP.

W. Wilson Randall, Susman Godfrey LLP, Houston, TX, for Dana Timaeus, Robert Rose.

[Craig Randal Lively](#), Harris Lively & Duesler, Beaumont, TX, [Frank H. Tomlinson](#), Pritchard McCall & Jones, Birmingham, AL, for Lindsey F. Tomlinson.

[Craig Randal Lively](#), Harris Lively & Duesler, Beaumont, TX, [Edward Cochran](#), Cochran & Cochran, Shaker Heights, OH, for Dan Gray, John Glase, Evan Morse, Betsy Melziner.

[Brent M. Langdon](#), Holman & Langdon LLP, Texarkana, TX, [Thomas C. Cronin](#), [Robert P. Cummins](#), Cummins & Cronin, Chicago, IL, for Deborah Cummins, Frank Pedote.

[R Stephen Griffis](#), Hooper & Griffis, Birmingham, AL, for David Skinner.

*[928 Laurence W. Schonbrun](#), Office of Laurence

Schonbrun, Berkeley, CA, for Robert Demyanovich.

[William H. Yoes](#), Law Offices of William H. Yoes, Beaumont, TX, [Robert W. Bishop](#), [Pamela G. Wilson](#), Bishop & Wilson, Louisville, KY, for Peyton T. Talbott, III.

ORDER DENYING MOTIONS FOR PARTIAL SUMMARY JUDGMENT

[HEARTFIELD](#), District Judge.

Before this Court are the *Motion by NEC Electronics, Inc. for Summary Judgment on Plaintiffs' Claims Under 18 U.S.C. § 1030 [56]* and *Defendant Toshiba America Information Systems, Inc.'s Motion for Partial Summary Judgment on 18 U.S.C. § 1030 and Brief in Support [58]*. Having considered the motions, the responses, the replies to the responses, and the arguments of counsel, this Court DENIES the *Motion by NEC Electronics, Inc. for Summary Judgment on Plaintiffs' Claims Under 18 U.S.C. § 1030 [56]* and *Defendant Toshiba America Information Systems, Inc.'s Motion for Partial Summary Judgment on 18 U.S.C. § 1030 and Brief in Support [58]*.

1. Facts and Procedural History

On March 5, 1999 Ethan Shaw and Clive D. Moon (collectively referred to as "Plaintiffs") filed this class-action complaint on behalf of themselves and all others similarly situated against Toshiba America Information Systems, Inc. ("Toshiba") and NEC Electronics, Inc. ("NECEL"). Why? Plaintiffs allege Toshiba and NECEL designed, manufactured, created, distributed, sold, transmitted, and marketed faulty, floppy-diskette controllers ("FDC's"). How are they faulty? "An FDC designed and manufactured pursuant to relevant specifications will detect data errors and allow the control program to rewrite the affected data correctly. The FDC's at issue in this case, instead, fail to detect the error, resulting in the storage of corrupt data or the destruction of data without the user's knowledge." *Plaintiffs' Second Amended Class Complaint [97]* 8. Plaintiffs dub this a "boundary error." Still a bit vague?

A properly designed and manufactured FDC that meets manufacturer specifications, however, will detect the boundary error conditions and assert an error status, which triggers the control program to rewrite the affected data correctly. Because of the defective microcode, Defendants' defective FDC's instead verify the erroneous data as correct without

an error status, resulting in the storage of corrupt data or the destruction of data without notice to the control program or operating system and without the operator's knowledge.

Local area network interface cards and sound cards are two examples of common DMA devices.

If a defective FDC is made to wait for data a few microseconds too long, because of competition for DMA, the defective FDC can cause corruption of data written to the attached device. If the wait for data is longer, a defective FDC can write the delayed data as the first byte [\[FN1\]](#) of the next physically adjacent data sector of a floppy diskette and destroy or "zero out" the remainder of data in that sector--all without reporting any error or notifying the control program or computer operator that data has been corrupted or destroyed. [\[FN2\]](#)

[FN1](#). A byte is an eight-bit segment of data. In typical computer usage, it usually represents one character, such as "A" or "z" or "7."

[FN2](#). So, the competition between a CD and a defective FDC for the DMA can cause the defective FDC to zero-out data.

Id. at 9-10. Indeed, the possibility of this boundary-error problem occurring increased when computers became capable of "multi-tasking"--that is, capable of performing several computer tasks at the same time. So Plaintiffs allege that if a computer is doing a bunch of stuff at the *929 same time the faulty FDC might stick the data in the wrong place; and it might stick it on top of other data which, consequently, gets messed up by the misplaced, over-written data. Finally, all of this data garbling goes undetected by the allegedly faulty FDC's; this, in turn, means it goes undetected by the person sitting in front of the computer. "Therefore, Defendants' FDC's are not capable of notifying the control program of data corruption. Worse yet, defective FDC's write corrupted data to the disk or other storage device and report to the computer operator that the data transfer was performed successfully." *Id.* at 10.

On July 15, 1999 NECEL filed its *Motion by NEC Electronics, Inc. for Summary Judgment on Plaintiffs' Claims Under 18 U.S.C. § 1030 ("NECEL's Motion for Summary Judgment") [56]* and Toshiba filed *Defendant Toshiba America Information Systems, Inc.'s Motion for Partial Summary Judgment on 18 U.S.C. § 1030 and Brief in Support ("Toshiba's Motion for Summary Judgment") [58]*. [\[FN3\]](#) In

these motions, NECEL and Toshiba urge this Court to grant partial summary judgment as to Plaintiffs' claims under [18 U.S.C. § 1030](#) since there is no "transmission" of code. In the alternative, Toshiba urges this Court to grant partial summary judgment as to Plaintiffs' claims under [18 U.S.C. § 1030](#) since Plaintiffs--as *current* owners of Toshiba's computers--are not entitled to injunctive relief that would theoretically benefit *future* buyers of Toshiba's computers. *Toshiba's Motion for Summary Judgment* [58] 1-2. Finally, NECEL also urges it is entitled to summary judgment since "[t]here simply is *no connection* between Plaintiffs and NECEL on which to base liability." [\[FN4\]](#) *Toshiba's Motion for Summary Judgment* [56] 2 (emphasis in original). NECEL's and Toshiba's motions endorse an overly restrictive view of [18 U.S.C. § 1030](#) and a misunderstanding of the standing requirement for the facts presented; [\[FN5\]](#) and NECEL's argument that there is "no connection" between it and the Plaintiffs is not entirely correct. So, the motions are denied.

[FN3.](#) On the same day NECEL filed its *Motion by NEC Electronics, Inc. for Summary Judgment on Plaintiffs' Claims for Breach of Contract, Breach of Warranty, and Revocation of Acceptance* [55]. This Court addresses NECEL's *Motion by NEC Electronics, Inc. for Summary Judgment on Plaintiffs' Claims for Breach of Contract, Breach of Warranty, and Revocation of Acceptance* [55] in a separate order.

[FN4.](#) The arguments presented by NECEL and Toshiba overlap considerably, but not completely. For example, both NECEL and Toshiba argue Plaintiffs fail to meet [Title 18 U.S.C. § 1030](#)'s requisite transmission since the statute was only intended to reach computer "hackers." However, Toshiba individually argues Plaintiffs do not have standing to seek their requested, injunctive relief; while NECEL individually argues there is "no connection" between it and the Plaintiffs.

[FN5.](#) A standing mis-understanding, if you will.

2. Summary Judgment Standard

[Rule 56\(b\) of the Federal Rules of Civil Procedure](#)

says: "A party against whom a claim, counterclaim, or cross-claim is asserted or a declaratory judgment is sought may, at any time, move with or without supporting affidavits for a summary judgment in the party's favor as to all or any part thereof." [Celotex Corp. v. Catrett](#), 477 U.S. 317, 324, 106 S.Ct. 2548, 2552, 91 L.Ed.2d 265 (1986). Furthermore, [Rule 56\(c\)](#) says, in part: "The judgment sought shall be rendered forthwith if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Thus, summary judgment is proper when, after a reasonable period for discovery, one party is unable to show a genuine issue as to a material fact on which he will bear the burden of proof at trial, provided that judgment against him is appropriate as a matter of law. [Nebraska v. Wyoming](#), 507 U.S. 584, 589, 113 S.Ct. 1689, 1694, 123 L.Ed.2d 317 (1993); [*930 Celotex](#), 477 U.S. at 322, 106 S.Ct. 2548. The moving party need not negate the elements of the non-moving party's case. [Id.](#) at 323, 106 S.Ct. 2548; [Little v. Liquid Air Corp.](#), 37 F.3d 1069, 1075 (5th Cir.1994) (en banc) (citing [Celotex](#), 477 U.S. at 323, 106 S.Ct. 2548, and [Lujan v. National Wildlife Fed'n.](#), 497 U.S. 871, 888, 110 S.Ct. 3177, 3188-89, 111 L.Ed.2d 695 (1990)). Rather, the moving party need only "demonstrate the absence of a genuine issue of material fact." [Celotex](#), 477 U.S. at 323, 106 S.Ct. 2548.

The non-moving party does not overcome the absence of a genuine issue of material fact by simply "creating some metaphysical doubt as to the material facts," [Matsushita Elec. Indus. Co. v. Zenith Radio Corp.](#), 475 U.S. 574, 586, 106 S.Ct. 1348, 1356, 89 L.Ed.2d 538 (1986), by making "conclusory allegations," [Lujan](#), 497 U.S. at 871-73, 110 S.Ct. 3177, by presenting "unsubstantiated assertions," [Little](#), 37 F.3d at 1075, or by proffering only a "scintilla" of evidence. *Id.* When the non-moving party fails to make a sufficient showing on an essential element of his case, the moving party is entitled to a judgment as a matter of law. *Id.* Nonetheless, when considering a motion for summary judgment, the trial court must construe all evidence in the light most favorable to the non-moving party and resolve all doubts against the moving party. [Eastman Kodak Co. v. Image Technical Servs., Inc.](#), 504 U.S. 451, 456, 112 S.Ct. 2072, 2076, 119 L.Ed.2d 265 (1992). With this standard in mind, this now Court turns to [Title 18 U.S.C. § 1030](#) (the "Computer Fraud and Abuse Act").

3. [Title 18 U.S.C. § 1030](#)--The Computer Fraud and Abuse Act

[Title 18 U.S.C. § 1030](#) is the "Computer Fraud and Abuse Act." Subsection 1030(a) (itself titled "Fraud and related activity in connection with computers") sets out the particular, substantive offenses proscribed by the statute. [\[FN6\]](#) As Toshiba notes, Plaintiffs (for whatever reason) do not specify which of the seven subsections of [§ 1030\(a\)](#) that Defendants allegedly violated. However, a brief review of the statute makes clear that *Plaintiffs' Second Amended Class Complaint* [97] could only purport to allege a violation of subsection 1030(a)(5). [\[FN7\]](#)

[FN6.](#) This particular statute was actually born in 1984 as the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984." [Pub.L. No. 98-473](#), 98 Stat. 2190. Prior to 1984, Congress relied on the mail and wire-fraud statutes to combat computer crime. However, the mail and wire-fraud statutes were often incapable of combating computer crime that did not involve interstate commerce. Thus, Congress enacted [Title 18 U.S.C. § 1030](#); and it amended it in 1986, 1988, 1989, 1990, 1994, and 1996.

[FN7.](#) As Toshiba points out, there simply are no allegations in *Plaintiffs' Original Class Complaint* [1] to support the violation of any other subsection of [§ 1030](#). Subsections 1030(a)(1) through 1030(a)(4) do not apply because each requires Defendants to have knowingly or intentionally "accessed" a computer without authorization (or exceeding the scope of authorization) and obtained sensitive information. [Title 18 U.S.C. § 1030\(a\)\(1\)-\(4\)](#). Moreover, there is no allegation that Defendants improperly obtained the specific types of information protected by subsections 1030(a)(1) through 1030(a)(4). *Id.* Subsection 1030(a)(6) does not apply because there are no allegations that Defendants intended to "traffic[] ... in any password or similar information through which a computer may be accessed without authorization." *Id.* Finally, subsection 1030(a)(7) does not apply because there are no allegations that Defendants intended to "extort ... any money or other thing of

value" and subsequently transmitted "any communication containing any threat to cause damage to a protected computer." *Id.* This leaves subsection 1030(a)(5)--and there are allegations to support the violation of this subsection.

Subsection 1030(a)(5)(A) says:

Whoever ... knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage [\[FN8\]](#) without authorization, to a protected ***931** computer [\[FN9\]](#) ... shall be punished in subsection (c) of this section.

[FN8.](#) "Damage" is the "any impairment to the integrity or availability of data, a program, a system, or information ..." that causes an aggregate loss of five thousand dollars (\$5,000.00) in a one-year period. [Title 18 U.S.C. § 1030\(e\)\(8\)](#).

[FN9.](#) A "protected computer" includes a computer "which is used in interstate or foreign commerce or communication." [Title 18 U.S.C. § 1030\(e\)\(2\)\(B\)](#).

[Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#). This is a criminal statute; however, [§ 1030](#) creates a private right of action for activity found to violate it:

Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.

[Title 18 U.S.C. § 1030\(g\)](#). So, this criminal statute creates a private right of action. [\[FN10\]](#) But does Defendants' activity arguably violate [Title 18 U.S.C. § 1030](#), thereby subjecting them to Plaintiffs' private right of action? Specifically, does [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#) prohibit Defendants' design, manufacture, creation, distribution, sale, transmission, and marketing of floppy-diskette controllers ("FDC's") allegedly made faulty by defective microcode? [\[FN11\]](#) Yes, it does.

[FN10.](#) Obviously, everyone concedes [Title 18 U.S.C. § 1030](#) creates a private right of action. The dispute lies in whether Defendants' activity falls under this statute--not whether a private right of action actually exists under it.

[FN11](#). Incidentally, for purposes of this summary judgment motion, NECEL concedes the existence of the boundary-error problem. See *NECEL's Motion for Summary Judgment* [56] 3 ("... for purposes of this summary judgment motion, it [NECEL] will concede an 'overrun' detection bug or defect.").

[\[1\]\[2\]\[3\]\[4\]](#) This Court's goal in interpreting the language of this particular statute--or any Congressional statute for that matter--is to give effect to Congress' intent. Not surprisingly, "[t]he starting point for interpreting a statute is the language of the statute itself." *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 102, 108, 100 S.Ct. 2051, 2056, 64 L.Ed.2d 766 (1980); see *Kennedy v. Texas Utilities*, 179 F.3d 258 (5th Cir.1999). The "inquiry must cease if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.'" *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340, 117 S.Ct. 843, 846, 136 L.Ed.2d 808 (1997) (citing *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 240, 109 S.Ct. 1026, 1030, 103 L.Ed.2d 290 (1989) and *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253-54, 112 S.Ct. 1146, 1149-50, 117 L.Ed.2d 391 (1992)). "Absent congressional direction to the contrary, words in statutes are to be construed according to 'their ordinary, contemporary, common meaning[s].'" *Kennedy*, *supra*, at 261 (quoting *Pioneer Inv. Servs. Co. v. Brunswick Assocs. Ltd. Partnership*, 507 U.S. 380, 388, 113 S.Ct. 1489, 1495, 123 L.Ed.2d 74 (1993) (quoting *Perrin v. United States*, 444 U.S. 37, 42, 100 S.Ct. 311, 314, 62 L.Ed.2d 199 (1979))). To interpret statutory terms, this Court examines "the statute as a whole, including its design, object, and policy." *New York Life Ins. Co. v. Deshotel*, 142 F.3d 873, 885 (5th Cir.1998); see *Adams Fruit Co. v. Barrett*, 494 U.S. 638, 642, 110 S.Ct. 1384, 1387, 108 L.Ed.2d 585 (1990). This Court defines particular terms with reference to the specific context in which they are used, *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340-41, 117 S.Ct. 843, 846-47, 136 L.Ed.2d 808 (1997); and it looks to the arrangement of certain terms within the statute as a guide to their meaning. See *Davis v. Johnson*, 158 F.3d 806, 811 (5th Cir.1998), *cert. denied*, --- U.S. ----, 119 S.Ct. 1474, 143 L.Ed.2d 558 (1999).

[\[5\]\[6\]\[7\]\[8\]](#) As Toshiba so eloquently notes, [\[FN12\]](#) "[f]idelity to the plain meaning of the text is not boundless." *Toshiba's Motion for Summary*

Judgment [58] 14. However, departure from the plain meaning of the text is not casually undertaken. If this Court "find[s] the terms of a statute unambiguous, judicial inquiry is complete, except in 'rare and exceptional circumstances.'" *[932](#) *Garcia v. United States*, 469 U.S. 70, 75, 105 S.Ct. 479, 482, 83 L.Ed.2d 472 (citing *TVA v. Hill*, 437 U.S. 153, 187 n. 33, 98 S.Ct. 2279, 2298, n. 33, 57 L.Ed.2d 117 (1978), quoting *Crooks v. Harrelson*, 282 U.S. 55, 60, 51 S.Ct. 49, 50, 75 L.Ed. 156 (1930)). Well what are those "rare and exceptional circumstances?" This Court must depart from the plain meaning of the statutory text if "it would lead to a result so bizarre that Congress could not have intended it." *Johnson v. Sawyer*, 120 F.3d 1307, 1319 (5th Cir.1997) (internal quotations omitted); see also *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571, 102 S.Ct. 3245, 3250, 73 L.Ed.2d 973 (1982); *United States v. A Female Juvenile*, 103 F.3d 14, 16-17 (5th Cir.1996) ("Axiomatic in statutory interpretation is the principle that laws should be construed to avoid an absurd or unreasonable result."). Also, when the statutory language is susceptible to more than one reasonable interpretation, this Court should look beyond the statutory text and examine the legislative history to divine congressional intent. *Uniroyal Chem. Co. v. Deltech Corp.*, 160 F.3d 238, 244 (5th Cir.1998); *Carpenters Dist. Council of New Orleans & Vicinity v. Dillard Dep't Stores, Inc.*, 15 F.3d 1275, 1283 (5th Cir.1994); *Dowling v. United States*, 473 U.S. 207, 213, 105 S.Ct. 3127, 3131, 87 L.Ed.2d 152 (1985) ("[W]hen assessing the reach of a federal criminal statute, we must pay close heed to language, legislative history, and purpose in order to strictly determine the scope of the conduct the enactment forbids ..."); accord *Crandon v. United States*, 494 U.S. 152, 157-58, 110 S.Ct. 997, 1001-1002, 108 L.Ed.2d 132 (1990) (the design, object, and policy of criminal statutes upon which civil liability is predicated is important evidence to consider). Look beyond to what? Should this Court determine that departure from the plain meaning of the text is warranted, it may look to official committee reports, conference reports, and contemporaneous statements by legislators on the committee that drafted the statute. See *North Haven Bd. of Educ. v. Bell*, 456 U.S. 512, 534, 102 S.Ct. 1912, 1924- 25, 72 L.Ed.2d 299 (1982); *Garcia v. United States*, 469 U.S. 70, 76, 105 S.Ct. 479, 482, 83 L.Ed.2d 472 (1984); *In re CompuAdd Corp.*, 137 F.3d 880, 883 (5th Cir.1998); *RTC v. Gallagher*, 10 F.3d 416, 421 (7th Cir.1993); *In re Kelly*, 841 F.2d 908, 912 n. 3 (9th Cir.1988). In addition to these sources beyond the statutory text, remarks by the legislative sponsors are deemed an "authoritative guide" to the meaning of the statute. *North Haven Bd. of Educ.*, 456 U.S. at 526-27, 102

[S.Ct. at 1920-21](#). Here, [Title 18 U.S.C. § 1030](#)'s language is unambiguous and its scheme is coherent and consistent. Thus, fidelity to the plain meaning of [Title 18 U.S.C. § 1030](#) is warranted--a plain meaning which encompasses Defendants' alleged activity.

[FN12](#). All parties submitted exceptional briefs.

1. Transmission or No Transmission? Transmission.

Both NECEL and Toshiba argue Plaintiffs have failed to state a cause of action under [Title 18 U.S.C. § 1030](#). Both Defendants argue the requisite "transmission" does not exist since a "transmission is not a code or command that originates and ends within a single computer." *See NECEL's Motion for Summary Judgment* [56] 16; *see also Toshiba's Motion for Summary Judgment* [58] 2. Plaintiffs respond that they "state a cause of action under [18 U.S.C. § 1030](#) by alleging in their First Amended Complaint that Defendants did in fact knowingly transmit **and are still transmitting** microcode or instructions contained in floppy disk controllers [FDC's], which microcode or instructions Defendants knew would cause the loss and corruption of data on computers used in interstate commerce." *Plaintiffs' Response to Toshiba America Information Systems Inc.'s Motion for Partial Summary Judgment Regarding [18 U.S.C. § 1030](#)* ("Plaintiffs' Response") [73] 6 (emphasis in original). How? "TAIS [Toshiba] still transmits the microcode in the laptop computers they sell *every day*. Each new sale of a Toshiba computer is a new knowing *933 transmission of this defective FDC code to another unsuspecting consumer." [\[FN13\]](#) *Id.* (emphasis in original). So, "for purposes of [18 U.S.C. § 1030](#), the issue is: **'Who caused the transmission of the microcode at issue in this lawsuit from its author in Japan to each of the Toshiba laptop computers in the United States.'**" *Id.* at 8 (emphasis in original). Well, under [18 U.S.C. § 1030\(a\)\(5\)\(A\)](#) does a "transmission" of microcode have to be *from one computer to another computer* --i.e., a "hacking" into another computer? Or may a "transmission" of microcode under [18 U.S.C. § 1030\(a\)\(5\)\(A\)](#) be *from the drafting of defective microcode and the subsequent sale of FDC's containing that microcode to consumers* --i.e., a marketing of FDC's allegedly made faulty by defective microcode?

[FN13](#). It is noteworthy that Defendants interpret "transmission" narrowly--with

particular emphasis on the technicalities of computer programming. On the other hand, Plaintiffs interpret "transmission" more broadly--with particular emphasis on the pragmatics of applying the statute to defendants' activity.

First, this Court notes that to "transmit" means, in plain English, "to send or convey from one person or place to another ... to cause or allow to spread ... to convey (infection) abroad or to another." *Webster's Collegiate Dictionary*, 10th ed. (1993). This is a rather broad definition--for it encompasses an inter-computer transfer of code (Defendants' argument), an intra-computer transfer of code (Defendants' initial interpretation of Plaintiffs' argument), [\[FN14\]](#) and a marketplace transfer of code (Plaintiffs' argument). That is, this definition of transmission would allow all three methods of "transmission" to potentially fall under [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#). However, merely opening the dictionary and quoting Webster would not follow the directives issued by the Supreme Court and the Fifth Circuit. The Supreme Court instructs this Court to define particular terms with reference to the specific context in which they are used. [Robinson v. Shell Oil Co.](#), 519 U.S. 337, 340-41, 117 S.Ct. 843, 846-47, 136 L.Ed.2d 808 (1997). Further, the Fifth Circuit directs this Court to look to the arrangement of certain terms within the statute as a guide to their meaning. *See Davis v. Johnson*, 158 F.3d 806, 811 (5th Cir.1998), *cert. denied*, --- U.S. ---, 119 S.Ct. 1474, 143 L.Ed.2d 558 (1999).

[FN14](#). Apparently, Defendants first read Plaintiffs' allegations as the requisite "transmission" occurring within a single computer as the defective microcode communicated with the FDC, which, in turn, improperly communicated to the attached device (i.e., the floppy disk). Subsequent briefing by Plaintiffs clarified that the requisite "transmission" encompassed the transmission of the defective microcode itself.

Thankfully, two other courts have already looked [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#) square in the eye--with particular focus on defendants' attempts to define themselves out of the statute via narrow construction of the term "transmission." The first case was [North Texas Preventative Imaging v. Eisenberg](#), 1996 WL 1359212 (C.D.Cal. August 19,

[1996](#). Plaintiff North Texas Preventative Imaging, L.L.C. ("NTPI") is a Dallas-based provider of medical diagnostic imaging (i.e., CAT scans), a method of diagnosing coronary artery disease, cancer, osteoporosis, and other medical conditions. In order to assist its diagnostic imaging, NTPI bought a computer system--the "Scribe system"--from defendant Medical Diagnostic Imaging, Inc. ("MDI"), a California-based company in the software business. The Scribe system performs computer enhancement of medical images. Plaintiff NTPI was dissatisfied with the Scribe system; and it sent Defendant MDI a letter "canceling" its purchase of the Scribe system and demanding return of the \$161,721.00 which had been "overpaid." Defendant MDI responded with a letter asking Plaintiff NTPI to enter into a new license agreement and noting that, if the new license were not executed, the software *934 (i.e., the Scribe system) would be disabled on January 31, 1996. When the software was initially installed, it contained no time restrictions or other disabling codes. However, Defendant MDI periodically sent Plaintiff NTPI "update disks" to keep the Scribe system current. In late 1995, Defendant MDI sent Plaintiff NTPI an "update" disk which, unbeknownst to Plaintiff NTPI, contained disabling codes--specifically, a "time bomb." "Disabling codes, or 'time bombs,' are computer software codes which render a software program inoperable at a pre-set time and date." *Id.* This 1995 "update disk" loaded one of these time bombs onto Plaintiff NTPI's computer--a time bomb set to go off January 31, 1996 and shut down the Scribe system. Before the time bomb went off, Plaintiff NTPI learned about its existence, complained to Defendant MDI, and secured an extension to the time bomb's clock. Then, Plaintiff NTPI sued Defendant MDI under various causes of action--one of which was a violation of [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#), the Computer Fraud and Abuse Act (the "CFAA").

Under a previous version of [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#)--a version arguably more favorable to Defendants than the current version [\[FN15\]](#)--the district court examined the legislative history and found:

[FN15](#). In 1994 [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#) read:
[Whoever] *through means of a computer used in interstate commerce or communications* knowingly causes the transmission of a program, information, code, or command to a computer or computer system ... [commits an offense if

other conditions are met]
[Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#) (1994 version) (emphasis added). In 1996 Congress amended subsection 1030(a)(5)(A) by deleting the qualifying phrase "through means of a computer used in interstate commerce or communications." Although this Court finds the statute unambiguous and an examination of the legislative history improper, it notes in passing that Congress' deletion of this qualifying phrase arguably removed the need for *computer-to-computer* "transmission."

By casting the net broadly to include many different "transmission" techniques, the 1994 amendment shifted the CFAA's focus from the act of unauthorized access to the intent of the defendant. The transmission of a disabling code by floppy computer disk may fall within the new language, if accompanied by the intent to cause harm.

Id. at *6. That is, the district court found "transmission" to include the development of destructive microcode in California, shipment of that destructive microcode via disk to a Dallas-based company, and downloading of that destructive microcode from the disk onto the Dallas-based company's computer. Defendant MDI had not "hacked" into Plaintiff NTPI's computers and installed the time bomb. Rather, Defendant MDI surreptitiously included the time bomb in one its regular "update disks" *that Plaintiff NTPI itself loaded onto its own computer*. Thus, [Title 18 U.S.C. § 1030](#)'s "transmission" included creation of destructive microcode in California, *the shipment of that destructive microcode via computer disk to Texas*, and the down-loading of that destructive microcode from the disk onto the computer in Texas.

The second case is *Gomar Manf. Co. v. Novelli, C.A. No. 96-4000* (D.N.J. Jan. 28, 1998). In that case, the district court (like this Court) faced a motion for partial summary judgment on the plaintiff's claims under the [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#), the Computer Fraud and Abuse Act. In May of 1994, Plaintiff Gomar Manufacturing Company, Inc. ("Gomar") bought a computer-controlled laminating machine from Defendant Geometric Machine & Design, Inc. ("Geometric"). Things got a little sticky when Plaintiff Gomar started having some problems with Defendant Geometric's laminating machine, and Defendant Gomar started having some problems with Plaintiff Gomar's payments (namely not getting them). Gomar alleged that, prior to delivery of the machine, Geometric *935 surreptitiously loaded a

"time bomb" onto the machine with a resettable trigger date which, if not continually advanced, would cause the laminating machine to malfunction. Gomar alleged that in November of 1995 the laminating machine--now victim to the exploded time bomb-- suddenly and repeatedly failed. Plaintiff Gomar sued Defendant Geometric under various causes of action--one of which was a violation of [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#), the Computer Fraud and Abuse Act (the "CFAA").

Under a previous version of [Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#)--again a version arguably more favorable to Defendants [\[FN16\]](#)--the district court examined the statutory language, the legislative history, and the *North Preventative* decision and found:

[FN16](#). *See supra.*, fn. 15.

no basis for concluding that disabling codes in the commercial context, even to prevent unauthorized use, are generally exempt from the CFAA. Senator Leahy's comments suggest, as the court in *North Texas [North Preventative]* concluded, that undisclosed disabling codes such as the disabling code at issue here were intended to be covered by the Act. That reading of the legislative history is consistent with the plain language of the Act as amended in 1994 to impose liability for damaging transmissions made "without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information or code or command ..."

Gomar Manf. Co. v. Novelli, C.A. No. 96-4000 (D.N.J. Jan. 28, 1998).

That is, the district court found "transmission" to include Defendant Geometric's loading of destructive microcode onto a computer laminating machine prior to the shipment and delivery of that laminating machine to Plaintiff Gomar. Defendant Geometric had not "hacked" into Plaintiff Gomar's computer laminating machine and installed the destructive microcode. Rather, Defendant Geometric actually loaded the destructive microcode onto the machine prior to the shipment and delivery of that machine to Plaintiff Gomar. Thus, [Title 18 U.S.C. § 1030](#)'s "transmission" included the shipment and delivery of pre- installed, destructive microcode, and the subsequent, automatic enablement of that pre- installed, destructive microcode.

First, this Court joins the *North Preventative* court in noting there are "very few cases which construe [18](#)

[U.S.C. § 1030](#) at all." [North Texas Preventative Imaging v. Eisenberg](#), 1996 WL 1359212 (C.D.Cal. August 19, 1996). Second, it joins the *North Preventative* and *Gomar* courts in their interpretations of the term "transmission" within [18 U.S.C. § 1030](#). The *North Preventative* court held [Title 18 U.S.C. § 1030](#)'s "transmission" included the creation of destructive microcode in California, *the shipment of that destructive microcode* via computer disk to Texas, and the down-loading of that destructive microcode from the disk onto the computer in Texas. The *Gomar* court held [Title 18 U.S.C. § 1030](#)'s "transmission" included the creation of destructive microcode, the installation of that destructive microcode on a laminating machine prior to delivery, *the shipment of pre- installed, destructive microcode* contained within that laminating machine, and the subsequent, automatic enablement of that pre- installed, destructive microcode. In this case, Plaintiffs argue [Title 18 U.S.C. § 1030](#)'s "transmission" includes *the shipment of defective microcode* subsequently contained within computer FDC's. This Court agrees. Both the *North Preventative* and *Gomar* courts refused to hog-tie the Computer Fraud and Abuse Act ("CFAA") (and, consequently, Congress) through unnecessarily narrow interpretations of "transmission." [\[FN17\]](#) *936 Now, so does this Court. [Title 18 U.S.C. § 1030](#)'s "transmission" includes the design, manufacture, creation, distribution, sale, transmission, and marketing of floppy-diskette controllers ("FDC's") allegedly made faulty by defective microcode.

[FN17](#). Again, although the statute is unambiguous and examination of the legislative history is improper, it notes in passing that Congress considered the fluid nature of computer crime and the difficulty in drafting a rigid law capable of catching all defendants with technical ingenuity and the requisite intent. In the 1989 subcommittee hearings, Senator Leahy noted "hidden programs can destroy and alter data." *The Impact of Computer Viruses and other Forms of Computer Sabotage and Exploitation on Computer Information Systems and Networks: Hearing Before the Subcommittee on Technology and the Law of the Committee on the Judiciary*, 101st Cong. (1989), at 1. He remarked: "You know, this is an area that changes all the time. Answers we have today may well be different a year or so from now. The questions, I am sure, will be different." 1989 Hearings, at 12.

Senator Leahy continued:

On the day that we pass a law, we are, in effect, taking a snapshot of what we know that day.

But however we draw it, somebody is going to sit down and say, well, look, I am just going to create a variation not covered by the statute. I am not sure all of us, putting our best minds together, could come up with every variation on a law that might get enacted some time this year to cover some new variation next year.

1989 Hearings, at 34.

[9] Toshiba argues Congress never intended the CFAA to reach manufacturers; rather, the CFAA is geared toward criminalizing computer "hacking." Setting the *North Preventative* and *Gomar* decisions aside, this Court does not see a blanket exemption for manufacturers in [Title 18 U.S.C. § 1030](#); nor does it see the term "hacking" anywhere in this statute. Again, Subsection 1030(a)(5)(A) says:

Whoever ... knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer ... shall be punished in subsection (c) of this section.

[Title 18 U.S.C. § 1030\(a\)\(5\)\(A\)](#). First, Toshiba argues:

Plaintiff's interpretation ... removes the requirement that it be the "transmission" that results in damage. According to Plaintiffs, the statute is violated if a component containing a bug in the microcode--which could cause "damage" to a computer no matter where the computer is located--is transported from one location to another ... Presumably ... a component that is not placed into interstate commerce, but which contains a bug in the microcode, would not give rise to liability, because there has ostensibly been no "transmission" of the component--even though the microcode could still "damage" the user's computer.

Defendant Toshiba America Information Systems, Inc.'s Reply to Plaintiffs' Response to TAIS' Motion for Partial Summary Judgment ("Toshiba's Reply")

[73] 4. Not necessarily. Toshiba urges an all or nothing interpretation of "transmission"--either transmission is wholly *outside computers* via marketplace transfer or wholly *inside computers* via inter-computer communication. [\[FN18\]](#) Well, if the requisite intent is there, why not both? "The principle of strict construction of criminal statutes does not mean that they must be given their narrowest possible meaning." [Singer v. United](#)

[States](#), 323 U.S. 338, 341-42, 65 S.Ct. 282, 284, 89 L.Ed. 285 (1945) (citing [United States v. Giles](#), 300 U.S. 41, 48, 57 S.Ct. 340, 344, 81 L.Ed. 493).

Toshiba argues that had Congress intended *937 for a marketplace transfer to fall under "transmission," "it would have used more specific words such as 'shipment' or 'transport' in place of 'transmission.'" Perhaps. But it seems more plausible that Congress, grappling with technology that literally changes every day, drafted a statute capable of encompassing a wide range of computer activity designed to damage computer systems--from computer hacking to time bombs to defective microcode. Next, Toshiba argues "Plaintiffs' reading is also incorrect because it would render meaningless subsection 1030(a)(5)'s use of the word 'command' ... A 'command' cannot be shipped or mailed from one location to another. If 'transmission' means shipping or mailing, it would be impossible to transmit a 'command.'" *Id.* Again, not necessarily. This argument, yet again, relies on an overly restrictive definition of "transmission." If the definition of "transmission" encompasses *both* a marketplace transfer and an electronic transfer of damaging *microcode*, [\[FN19\]](#) then it is indeed possible to "transmit" a command. [\[FN20\]](#)

[FN18](#). For example, Defendants argue a computer that contains destructive microcode could avoid having "transmitted" the microcode if the computer is never *shipped* in interstate commerce. Aside from the fact that this hypothetical computer necessarily moved in interstate commerce prior to the transmission of the damaging microcode, the emphasis should be on the transmission of the destructive microcode--not the physical location of the computer that contains it. If the destructive microcode is transmitted to or from that computer by a defendant with the requisite intent, then such activity would properly fall under the statute regardless whether the defendant actually put the computer in his car and drove it up and down the interstate highway across state lines.

[FN19](#). Toshiba alternatively argues that even if a code or command within a single computer constitutes a "transmission," the FDC's allegedly "*failed* to send code or commands to other components ... [and][a] 'transmission' is not a failure to send a particular code or command." *Id.* Again, the emphasis should be on the transmission of

the damaging microcode, whether it be in the form of a floppy disk loaded with destructive microcode, a laminating machine loaded with destructive microcode, or FDC's loaded with destructive microcode. The reason the FDC "failed" to send code to other components is because defective microcode was allegedly authored in Japan and transmitted to computers in the United States.

[FN20](#). And lo, the hog is set free.

2. Plaintiffs Have Standing.

[\[10\]](#) Plaintiffs seek an injunction requiring Toshiba "to advise all potential purchasers that computers they have manufactured can corrupt and destroy data without warning ..." *Plaintiffs' Second Amended Complaint* [97] 13. Toshiba argues Plaintiffs do not have standing to seek this requested, injunctive relief. "[N]either of the two named Plaintiffs are 'potential' purchasers; both have allegedly purchased computers manufactured by one or both of the defendants. As a result, Plaintiffs do not have standing to seek injunctive relief on behalf of 'potential purchasers' of the defendants' computers." *Toshiba's Motion for Summary Judgment* [58] 21.

Plaintiffs respond that [Title 18 U.S.C. § 1030\(g\)](#) specifically authorizes their request for injunctive relief:

any person who suffers damage or loss by reason of a violation of the section ... may maintain a civil action against the violator to obtain compensatory damages and *injunctive relief* or other equitable relief.

[Title 18 U.S.C. § 1030\(g\)](#) (emphasis added). But authorization for injunctive relief and standing to assert it are not one in the same. To bring a claim for injunctive relief, a plaintiff must "show that he 'has sustained or is immediately in danger of sustaining some direct injury' as a result of the challenged ... conduct." *Armstrong v. Turner Indus., Inc.*, 141 F.3d 554, 563 (5th Cir.1998) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 102, 103 S.Ct. 1660, 1665, 75 L.Ed.2d 675 (1983)). Moreover, "[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief ... if unaccompanied by any continuing, present adverse effects." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564, 112 S.Ct. 2130, 2138, 119 L.Ed.2d 351 (1992) (quoting *O'Shea v. Littleton*, 414 U.S. 488, 495-96, 94 S.Ct. 669, 676, 38 L.Ed.2d 674 (1974)).

Here, Plaintiffs have both authority to seek injunctive relief and standing to assert it. First, Plaintiffs are presently in the pool of prospective purchasers of Defendants' personal computers. Apparently, Toshiba would have this Court hold Plaintiffs do not have standing to assert a *938 claim under [Title 18 U.S.C. § 1030](#) as "potential purchasers" merely because they already purchased Defendants' computers. But Plaintiffs' proposed class includes "potential purchasers" for a very simple reason: had Plaintiffs' proposed class sought to include "current owners" of Toshiba computers, Defendants could simply argue Plaintiffs lack standing to seek the requested relief of notice since they *already know about the allegedly defective FDC* (for how else could they complain about the defect if they didn't already know about it?). To prevent this catch--22, the proposed class includes "potential purchasers," and Plaintiffs are precisely that--potential purchasers of Defendants' computers. [\[FN21\]](#) More important, Plaintiffs' exposure to the allegedly corrupted data from other Toshiba computers is ever present. Plaintiffs allege:

[FN21](#). It goes without saying (or maybe not) that Plaintiffs, although *current* owners of Defendants' computers, may indeed be *future* purchasers of other computers containing FDC's allegedly infected with the defective microcode.

The damage caused by the FDC's faulty microcode would include an impairment of the integrity or availability of data, or information that impairs or potentially impairs the medical examination, diagnosis, treatment, or care of one or more individuals or threatens the public health or safety. When doctors cannot trust the medical data in their computers or the test results they receive from the lab; when engineers cannot depend on the data they use to design our bridges, skyscrapers, dams, and commercial airliners, Defendants pose a clear risk to public health and safety.

Plaintiffs' Response to Toshiba's Motion for Summary Judgment [73] 23. Toshiba is currently the number-one provider of laptop computers in the United States. Toshiba's dominance of the computer market, combined with the considerable penetration of the defective microcode into computers via the ubiquitous FDC's allegedly containing the defective microcode, ensures Plaintiffs' exposure to the effects of faulty data allegedly generated by Defendants' conduct. It is unnecessary for someone to *lack* a computer in order to be a "potential purchaser" of

one. Similarly, it is not necessary for someone to actually *own* a defective computer in order to experience continuing, adverse effects from it. [\[FN22\]](#)

[FN22.](#) If the nay-sayers and army surplus vendors are right, just wait until Y2K to see this proposition proven true with a vengeance.

3. *NECEL's Connection to the Plaintiffs--Computer History 101.*

NECEL joins Toshiba in arguing [Title 18 U.S.C. § 1030](#)'s application reaches only computer "hackers" and not manufacturers; but it departs Toshiba in arguing "[t]here simply is *no connection* between Plaintiffs and NECEL on which to base liability." *NECEL's Motion for Summary Judgment* [56] 2 (emphasis in original). NECEL is a California corporation in the business of selling semiconductor devices manufactured by its parent corporation, NEC Corporation of Tokyo, Japan ("NECTOK"). NECEL has sold FDC's, but never to Toshiba or any Toshiba affiliate. NECEL has never designed an FDC; and, except for packaging, it has never manufactured an FDC. So what's NECEL doing in this lawsuit?

NECTOK first produced the (micro)PD765 FDC in 1978--the dawn of the computer age. Apple, Commodore, and Tandy had just introduced the personal computer in 1977; and IBM would not enter the personal computer market for another three years. In December of 1986, NECTOK first became aware of the boundary-error problem within its (micro)PD765 FDC--which by then included model numbers (micro)PD765A, (micro)PD765A-2, and 72065 (collectively referred to as the "A-version FDC's"). [\[FN23\]](#) In *939 March 1987, NECTOK notified NECEL's largest customer, IBM, of the boundary-error problem and NECTOK's plan to fix it. [\[FN24\]](#) On October 2, 1987 NECTOK and its overseas affiliates notified all FDC customers of the boundary-error problem. They also posted notice on NECTOK's communications network and later on its website, <[http:// nesdisw.ic.nec.co.jp](http://nesdisw.ic.nec.co.jp)>, where it remains today in both Japanese and English. Then, in late 1987, NECTOK produced the "B-version" of the (micro)PD765 FDC--a version which fixed the boundary-error problem experienced by the "A-version" FDC's. Volume production of the new "B-version" of the (micro)PD765 FDC ((micro)PD765B and 72065B) began in 1988. But some customers elected to continue using the "A-version" FDC's,

understanding they needed to keep their systems within certain timing specifications to avoid the boundary-error problem still contained within their older, "A-version" FDC's driven by the defective microcode. [\[FN25\]](#)

[FN23.](#) NECEL calls the boundary-error problem an "overrun detection defect or bug." See *NECEL's Motion for Summary Judgment* [56] 3. For simplicity, this Court will continue to refer to the defect as a "boundary- error problem." See *supra*, pp. 928-29.

[FN24.](#) Why IBM? The boundary-error problem was particularly important to IBM since it was working on the OS/2 operating system--a system capable of multi-tasking and, consequently, increasing the possibility for the boundary-error problem to occur. See *supra*, p. 929.

[FN25.](#) Specifically, customers continuing to use the defective "A- version" FDC's needed to keep their systems' data request ("DRQ")--data acknowledgment ("DACK") signals strictly within the NEC timing specifications. The NEC User's Manuals for the (micro)PD765A/765B and (micro)PD765/72065B explained the boundary-error problem in the "A-version" FDC's and cautioned customers to stay within NEC's timing specifications.

In 1990 NECEL began marketing its latest "B-version" of NECTOK's FDC (embodied in the further improved (micro)PD72064) as multitasking [\[FN26\]](#) ready, whereas its imitators were not. In November 1990 NECEL launched a colorful "Multitasking Murder Mystery" advertising campaign that warned computer-system manufacturers that some "765-compatible" FDC's had a "killer bug" that could result in "Dastardly deeds done in disk drives." For customers moved by the ad, NECEL provided a diagnostic disk to test whether the FDC's they were using had the defective microcode and, consequently, were subject to the boundary- error problem. The solution, of course, was to switch to NEC's new FDC's which did not have the defective microcode and, consequently, were capable of taking on the challenges of multitasking. The advertising campaign ended in November of 1991; and NECEL

sold its last batch of "Aversion" FDC's in 1993, when it sold two hundred and thirty (230) pieces. Today, NECEL makes only semiconductors containing the "B-version" FDC's. As for the older "A-version" FDC's, NECEL merely keeps a few, old parts to provide replacements to customers who continued to use the "A-version" FDC's despite the boundary-error problem. So, it *seems like* NECEL should not be in this lawsuit. So it *seems* ...

[FN26](#). See *supra*, p. 929.

NECEL's 765 FDC's were immensely popular in the 1980's; and NECEL suspected many companies, like Toshiba, were copying the NECTOK (micro)PD765 FDC. So, in 1985 NECTOK accused Toshiba of illegally copying its (micro)PD765 FDC; of course, Toshiba denied this allegation. But in 1986 NECTOK and Toshiba executed an agreement settling their dispute. This agreement provided that neither would sue or assert its patent, copyright, or maskwork rights against the other's FDC's specified in the agreement. [\[FN27\]](#) Under this "antipirating-type agreement," Toshiba agreed to pay NECTOK an eight percent (8%) royalty on its internal and external sales of specified FDC's. Later, in *940 1989, the parties amended the agreement to include Toshiba's newer FDC's and provided a royalty of seven percent (7%) for Toshiba's newer FDC's and semiconductors based on the accused, pirated core. Of course, as NECTOK's chips were allegedly "pirated" by Toshiba, NECEL did not provide any FDC designs to Toshiba; nor did NECEL review or approve any Toshiba designs; nor did NECEL test any FDC's for Toshiba; nor did NECEL permit Toshiba to put the NEC name on any Toshiba products or authorize Toshiba to represent that its FDC's were "NEC-compatible" or "765-compatible."

[FN27](#). Plaintiffs' counsel, Mr. Hubert Oxford, accurately described the NECTOK-Toshiba agreement as a "you won't sue me for using these chips, an antipirating-type agreement." *Transcript of June 24, 1999 Hearing on Objections to Initial Disclosures* at p. 31, ll. 14-15.

[\[11\]\[12\]](#) So, is there a connection between NECEL and the Plaintiffs? Yes, there is. At this point it's necessary to return to the statute at issue in this litigation--[Title 18 U.S.C. § 1030](#). This is a criminal statute. "It is a general principle of causation in

criminal law that an individual (with the necessary intent) may be held liable if he is a cause in fact of the criminal violation, even though the result which the law condemns is achieved through the actions of innocent intermediaries." [United States v. Kelner](#), 534 F.2d 1020, 1022 (2nd Cir.), cert. denied, 429 U.S. 1022, 97 S.Ct. 639, 50 L.Ed.2d 623 (1976) (citing [United States v. Giles](#), 300 U.S. 41, 48-49, 57 S.Ct. 340, 344, 81 L.Ed. 493, 497-98 (1937); [United States v. Scandifia](#), 390 F.2d 244, 249 (2nd Cir.1968), vacated on other grounds sub. nom., [Giordano v. United States](#), 394 U.S. 310, 89 S.Ct. 1163, 22 L.Ed.2d 297 (1969); [King v. United States](#), 364 F.2d 235, 238 (5th Cir.1966) ("There are, of course, many instances in which violations of the law are brought about by one who intentionally causes another to unwittingly perform the prohibited act.")). An intervening act, tortious or criminal, will insulate a defendant from liability only when the defendant could not have reasonably anticipated the subsequent act. [Cullen v. BMW of North America, Inc.](#), 691 F.2d 1097, 1101 (2nd Cir.1982), cert. denied, 460 U.S. 1070, 103 S.Ct. 1525, 75 L.Ed.2d 948, (1983); accord [United States v. Sneed](#), 63 F.3d 381 (5th Cir.1995).

[\[13\]](#) NECEL seeks exclusion from this lawsuit because it never designed, manufactured, or owned any intellectual property rights to any *FDC* design. Well that's a red herring. The issue in this case is not the transmission of FDC's--it's *the transmission of defective microcode* subsequently contained within the FDC's. NECEL's incredible success with its "A-version" FDC's--FDC's containing the allegedly defective microcode--apparently spawned copy-cat versions themselves containing the defective microcode. Indeed, the "anti-pirating" agreement between NECTOK and Toshiba fosters the continued transmission of the defective microcode to this very day. Apparently, NECTOK and, most likely, NECEL have profited and continue to profit from the royalties earned from the NECTOK-Toshiba "antipirating" agreement. Regardless whether NECTOK and NECEL profited from the sale of FDC's allegedly containing the defective microcode, it seems most plausible that NECTOK and NECEL could have foreseen the transmission of the defective microcode via the marketplace transfer of FDC's *containing the very same, defective microcode NECTOK had just claimed was "illegally copied" from it by Toshiba*. [\[FN28\]](#) So NECEL did not provide any FDC designs to Toshiba; so NECEL did not review or approve any Toshiba designs; so NECEL *941 did not test any FDC's for Toshiba; so NECEL did not permit Toshiba to put the NEC name on any Toshiba products or authorize Toshiba to represent that its

FDC's were "NEC-compatible" or "765-compatible." So what. NECTOK and NECEL could have foreseen the transmission of the defective microcode via the marketplace transfer of FDC's *containing the very same, defective microcode NECTOK had just claimed was "illegally copied" from it by Toshiba*. The fact that an intermediary--Toshiba (be it innocent or not)--was used to allegedly violate [Title 18 U.S.C. § 1030](#) does not relieve NECEL from liability since it could have reasonably anticipated the subsequent transmission of the defective microcode. [\[FN29\]](#)

[FN28](#). How convenient for NECTOK to create, and NECEL to market, the "A-version" FDC's with defective microcode, have those FDC's copied by competitors, and enter into antipirating-type agreements to actually get paid for competitors using defective microcode that NECTOK and NECEL created and marketed. How even more convenient for NECTOK and NECEL to detect the boundary-error problem, correct it with its new "B-version" FDC's, and market these new "FDC's as correcting the 'competitors' " boundary-error problem amplified by the development of multitasking--a boundary-error problem *that NECTOK and NECEL created, marketed, and passed on to its competitors*. All of sudden the "Multitasking Murder Mystery" is not such a mystery after all.

[FN29](#). Indeed, not only could NECEL have *anticipated* the subsequent transmission of the defective microcode, it had proof-positive that transmission had occurred. How's that? The only way NECTOK and NECEL could get royalty checks from Toshiba would be for the sale of FDC's--FDC's that allegedly contained the "illegally-copied," defective microcode created by NECTOK and marketed by NECEL. In a way, Toshiba actually paid NECTOK and NECEL to transmit defective microcode. NECEL argues it would not intentionally market this defective microcode since, to do so, would be "suicide" in the computer market. Well, as NECEL points out, it was Toshiba's name plastered all over the FDC's allegedly containing the defective microcode. NECEL, in the business of selling laptop computers, wants to sell *more* of those laptop computers. If Toshiba's (and other

competitors') sale of computers falls due to a reputation damaged by concern over FDC's allegedly made faulty by defective microcode (defective microcode created and passed on by NECTOK and NECEL, nonetheless), then NECEL gets to sell that many more laptop computers, all while touting the superiority of its "B-version" FDC's in light of the inferior "A-version" FDC's which, although created by NECTOK and marketed by NECEL, have the Toshiba name plastered all over it. Certainly, the White Star Line would have happily painted "Carnival Cruise Lines" all over the Titanic had it known the ship's rudder was too small, there were too few lifeboats, and the captain was going to speed in the dark of night through the Atlantic shipping lane which, at that time, was an impassable slalom course of icebergs.

4. Conclusion

First, NECEL's and Toshiba's motions endorse an overly restrictive view of [Title 18 U.S.C. § 1030's](#) "transmission." "Transmission" includes the design, manufacture, creation, distribution, sale, transmission, and marketing of floppy-diskette controllers ("FDC's") allegedly made faulty by defective microcode. Setting the *North Preventative* and *Gomar* decisions aside, this Court refuses to hog-tie [Title 18 U.S.C. § 1030](#)--and, consequently, Congress--with overly restrictive, statutory interpretations generated by semantic parsing designed to inject technicalities where none exist. Further, Toshiba's motion reflects a misunderstanding of the standing requirement for the facts presented. Toshiba's dominance of the computer market, combined with the considerable penetration of the allegedly defective microcode into these computers via the FDC's, ensures Plaintiffs' exposure to the effects of faulty data allegedly generated by Defendants' conduct--regardless whether Plaintiffs currently own one of Defendants' computers, are thinking about buying one of Toshiba's computers, or are commuting to work over a bridge with design specifications tainted by allegedly faulty FDC's misguided by the defective microcode. Finally, NECEL's argument that there is "no connection" between it and the Plaintiffs is simply incorrect. NECEL marketed defective microcode which its parent, NECTOK, generated. According to NECEL, Toshiba "illegally copied" this defective microcode and incorporated it into its FDC's. As a result of the popularity of its "A-version" FDC's, NECTOK

executed a royalty agreement which actually rewarded NECTOK and, quite possibly, NECEL for the transmission of the allegedly faulty microcode--albeit under the guise of the Toshiba name. Even if NECEL did not profit from this royalty agreement, it most likely benefitted from Toshiba's decreased sales hampered by the sale of computers with defective microcode *942 initially generated by NECTOK, marketed by NECEL, and then "fixed" by NECTOK's "B-version" FDC's marketed by NECEL as correcting a problem that, in reality, NECTOK had created and NECEL had marketed.

For these reasons, this Court DENIES the *Motion by NEC Electronics, Inc. for Summary Judgment on Plaintiffs' Claims Under 18 U.S.C. § 1030 [56]* and *Defendant Toshiba America Information Systems, Inc.'s Motion for Partial Summary Judgment on 18 U.S.C. and Brief in Support [58]*.

It is SO ORDERED.

91 F.Supp.2d 926

END OF DOCUMENT