

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF LOUISIANA**

**PHILLIP BECKER, ET AL.**

**CIVIL ACTION**

**VERSUS**

**NUMBER 07-7202**

**MARY MICHELLE MCINTYRE TOCA**

**SECTION "L" (3)**

**ORDER & REASONS**

Before the Court is the Defendant's Motion to Dismiss (Rec. Doc. 16). For the following reasons, the Defendant's motion is now GRANTED IN PART AND DENIED IN PART.

**I. BACKGROUND**

On October 23, 2007, the Plaintiff, a lawyer, initiated this action against the Defendant, his ex-wife, for punitive damages, attorney fees, injunctive relief, and equitable relief pursuant to (1) the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*; (2) the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* ("SCA"); (3) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(5)(a)(i), *et seq.*; and (4) the Louisiana Electronic Surveillance Act, La. Rev. Stat. 15:1302, *et seq.* The Plaintiff alleges that the Defendant installed a computer virus on his office and personal computers in order to steal his passwords and gain access to financial information for leverage in their ongoing divorce proceedings.

According to the Plaintiff, who operates a law firm in Lake Charles, Louisiana, he and his staff "began to experience considerable difficulties in both their home and office computers." Compl. ¶ 6. The Plaintiff alleges that the difficulties included "error messages, slow processing, and other indicators of technical problems with the operations of the computers." *Id.* The

Plaintiff further alleges that he retained the services of Webtronics, a computer repair company, in order to run diagnostic operations on his computers. The Plaintiff reports that Webtronics identified “spyware and viruses on two Compaq computers and one Toshiba laptop which were severe in nature.” *Id.* ¶ 8.

The Plaintiff claims that, “[u]pon further examination, it became apparent that the computers in question were infected with an internet ‘Trojan Horse’ virus named ‘Infostealer.’” *Id.* ¶ 9. According to the Plaintiff, the Infostealer program is “used to detect and steal passwords from computers operated by others, and works by gathering the passwords from the compromised computer and sending them to a remote computer by email or other means.” *Id.* The Plaintiff alleges that the Defendant intentionally sent the Infostealer program to him “by means of various emails and attachments” in order to gain financial information for use in the ongoing divorce proceedings between the two. *Id.* ¶¶ 10, 11.

## **II. PRESENT MOTION**

On March 24, 2008, the Defendant filed a Motion to Dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. The Defendant contends that the Plaintiff’s allegations fail to state a valid claim under each of the statutes by which the Plaintiff seeks relief. First, the Defendant argues that sending a computer virus to detect and steal passwords located on a computer does not constitute an attempt to “intercept” an “electronic communication” for purposes of the Federal Wiretap Act. Second, the Defendant argues that the Stored Communications Act does not apply to the instant case because the Plaintiff’s computers are not “facilit[ies] through which an electronic communication service is provided.” Third, the Defendant argues that the Computer Fraud and Abuse Act does not apply because the Plaintiff

only alleges that the Defendant sought to recover passwords and did not intend to “harm” the Plaintiff’s computer. Finally, the Defendant argues that the Louisiana Electronic Surveillance Act does not apply because that statute only prohibits the interception of “wire or oral” communications.

### **III. LAW & ANALYSIS**

“The district court may not dismiss a complaint under rule 12(b)(6) ‘unless it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief.’ “ *Lowrey v. Texas A & M Univ. Sys.*, 117 F.3d 242, 247 (5th Cir.1997) (quoting *Conley v. Gibson*, 355 U.S. 41, 45-46 (1957)). The Court must construe the complaint liberally in favor of the plaintiff, “and all facts pleaded in the complaint must be taken as true.” *Campbell v. Wells Fargo Bank*, 781 F.2d 440, 442 (5th Cir.1986). “In order to avoid dismissal for failure to state a claim, however, a plaintiff must plead specific facts, not mere conclusory allegations.” *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498 (5th Cir.2000) (quoting *Tuchman v. DSC Commc'ns Corp.*, 14 F.3d 1061, 1067 (5th Cir.1994)). “Factual allegations must be enough to raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true (even if doubtful in fact).” *Bell Atlantic Corp. v. Twombly*, 127 S. Ct 1955, 1965 (2007). The Court will address each of the Defendant’s arguments in turn.

#### **A. The Federal Wiretap Act**

The Federal Wiretap Act subjects to criminal liability any person who “intentionally intercepts [or] endeavors to intercept ... any wire, oral or electronic communication,” except as

otherwise permitted by law. 18 U.S.C. § 2511(1)(a). “Electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12).

“Intercept” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). The Wiretap Act provides a civil cause of action for persons whose electronic communications are intercepted in violation of its provisions. 18 U.S.C. § 2520.

In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the Fifth Circuit held that the government did not “intercept” electronic communications by seizing a computer containing unread email messages stored on an electronic bulletin board system. In examining the scope of the Federal Wiretap Act, the court noted as significant the fact that Congress had defined wire and electronic communications differently:

Critical to the issue before us is the fact that, unlike the definition of ‘wire communication,’ the definition of ‘electronic communication’ does not include electronic storage of such communications.... Congress’ use of the word ‘transfer’ in the definition of ‘electronic communication,’ and its omission in that definition of the phrase ‘any electronic storage of such communication’ ... reflects that Congress did not intend for ‘intercept’ to apply to ‘electronic communications’ when those communications are in ‘electronic storage.’

*Id.* at 461-62. As a result, the court held that the e-mail messages stored on the BBS’ computer hard drive were no longer in transmission and thus could not be “intercepted” within the meaning of the Wiretap Act. *Id.* at 461.

Several courts that have since considered the issue have endorsed the Fifth Circuit’s interpretation that the definition of “intercept” encompasses “only acquisitions contemporaneous

with transmission.” *United States v. Seiger*, 318 F.3d 1039, 1047 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2001). For example, in *Bailey v. Bailey*, 2008 WL 324156, \*5 (E.D. Mich. 2008), the court granted the defendant’s motion for summary judgment, holding that the Wiretap Act did not apply to the defendant’s installation of a Trojan Horse program on his wife’s computer in order to steal her email messages and passwords. In finding the Wiretap Act inapplicable, the court in *Bailey* carefully examined the mechanics of the Trojan Horse program and concluded that the defendant had not “obtain[ed] the emails or messages contemporaneously with their transmission.” *See id.*; *see also Steiger*, 318 F.3d at 1050 (“[T]he evidence shows that the source used a Trojan Horse virus that enabled him to access and download information stored on Seiger’s personal computer. This conduct, while possibly tortious, does not constitute an interception of electronic communications in violation of the Wiretap Act.”).

Turning to the instant case, the Court finds that the Plaintiff’s claims under the Federal Wiretap Act cannot be dismissed at this time. The Plaintiff alleges that the Defendant installed a Trojan Horse program on his computer “to detect and steal passwords ... by gathering the passwords from the compromised computer and sending them to a remote computer by email or other means.” Compl. ¶ 9. The Plaintiff further alleges that he used his computers in connection with his business and that the computers were “connected to the Internet by typical means.” *Id.* ¶ 5. Assuming that the Plaintiff’s allegations are true, it is reasonable at this time to infer that the Trojan Horse program may have collected information contemporaneous to its transmission over the internet. Although the Plaintiff may ultimately face considerable difficulties demonstrating that the claims should survive summary judgment, it would be premature and speculative for the Court to dismiss the claims at this time.

## **B. The Stored Communications Act**

The Stored Communications Act (“SCA”) subjects to criminal liability any person who

intentionally accesses without authorization a facility through which an electronic communication service is provided [and] thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.

18 U.S.C. 2701, *et seq.* The statute defines an “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1) of the SCA). “Electronic storage” is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and [] any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. §§ 2510(17)(A), (B). The SCA provides that a civil action may be brought “by any provider of electronic communication service, subscriber, or other person aggrieved by a violation ... in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind.” 18 U.S.C. § 2707.

Courts have interpreted the statute to apply primarily to telephone companies, internet or e-mail service providers, and bulletin board services. *See Steiger*, 318 F.3d at 1049; *Steve Jackson Games*, 36 F.3d at 462-63; *see also In re DoubleClick, Inc. Privacy Litig.*, 154 F.Supp.2d 497 (S.D.N.Y. 2001) (finding that the SCA did not prohibit websites from placing ‘cookies’ on personal computers because, *inter alia*, the personal computers at issue were not “electronic communication service providers.”)<sup>1</sup> For example, an online business or retailer

---

<sup>1</sup>In *DoubleClick*, the court went on to explain that “[e]xamples of providers in the Internet world would include ISPs such as America Online, Juno and UUNET, as well as, perhaps, the telecommunications companies whose cables and phone lines carry the traffic.” *In re*

may be considered an electronic communication service provider if the business has a website that offers customers the ability to send messages or communications to third parties. *Compare Kaufman v. Nest Seekers, LLC*, 2006 WL 2807177, \*6 (S.D.N.Y. 2006) (“An on-line business which provides its customers, as part of its commercial offerings, the means by which the customers may engage in private electronic communications with third-parties may constitute a facility through which electronic communication service is provided.”) *with Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal 2001) (holding that an online merchant with a website that only allows customers to send electronic communications directly to the merchant does not provide electronic communication services within the contemplation of the SCA).

In *United States v. Steiger*, the court held that the SCA did not prohibit an anonymous source from installing a Trojan Horse virus on the defendant’s computer in order to search his hard drive for evidence of child pornography. 318 F.3d at 1049. The court explained that the “SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board service (BBS).” *Id.* In contrast, however, the court explained that the SCA “does not appear to apply to the source’s hacking into Steiger’s computer to download images and identifying information stored on his hard drive.” *Id.* The court found persuasive the fact that the Defendant had not presented any evidence that his computer “maintained any ‘electronic communication service’ as defined in 18 U.S.C. § 2510.” *Id.* The court noted, however, that “the SCA may apply to the extent the source accessed and retrieved

---

*Doubleclick*, 154 F. Supp. 2d at 511 n.20. The court further noted that “the section is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it.” *Id.* at 512.

any information stored with Steiger's internet service provider." *See id.*; *see also Bailey*, 2008 WL 324156, \*6 (explaining that protection under the SCA "does not extend to emails and messages stored only on Plaintiff's personal computer").

Turning to the instant case, the Court finds that the Plaintiff's claims under the SCA cannot be dismissed at this time because it is unclear to what extent the program may have accessed or retrieved information stored with an electronic communication service provider. Although the Plaintiff does not allege that his personal or office computers were "facilities through which an electronic communication service is provided," the computers may qualify as such because the Plaintiff does allege that he used the computers to run his business. Further, the Plaintiff alleges that the Defendant transmitted the Trojan Horse program to him via email and that the program sent information back to the Defendant "by email or other means." It is therefore unclear whether the program may have accessed files stored with an electronic service provider during its transmission of data. Finally, the Plaintiff alleges that the Trojan Horse program targeted passwords, and it is unclear to the Court whether the targeted passwords were system passwords saved on the Plaintiff's hard drive or web-based passwords captured during transmission over the internet. Although the Plaintiff may face considerable difficulties in demonstrating that the SCA claim should survive summary judgment, it would be premature and speculative for the Court to dismiss the claim at this time.

### **C. The Computer Fraud and Abuse Act**

The Computer Fraud and Abuse Act subjects to criminal liability any person who

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



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

18 U.S.C. § 1030(a)(5)(A)(i). The statute defines a “protected computer” as a computer “which is used in interstate ... commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). “Damage” is defined as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). “Loss” is defined as “any reasonable cost to any victim, including the cost of responding to an offense, conducting damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). In addition to subjecting any person who violates the statute to criminal liability, the statute also provides a civil remedy for any person who suffers damage or loss resulting from such a violation. 18 U.S.C. § 1030(g).<sup>2</sup>

The Defendant makes two arguments as to why the Plaintiff’s complaint fails to state a claim under the Computer Fraud and Abuse Act. First, the Defendant argues that the Plaintiff

---

<sup>2</sup>Pursuant to 18 U.S.C. § 1030(g), the statute only provides a civil remedy against a person whose conduct caused or, if completed, would have caused:

- (i) loss to 1 or more persons during any 1-year period ... aggregating at least \$5,000 in value;
- (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
- (iii) physical injury to any person;
- (iv) a threat to public health or safety; or
- (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

18 U.S.C. §§ 1030(a)(5)(B), 1030(g). If the person’s conduct caused or would have only caused “loss to 1 or more persons during any 1-year period ... aggregating at least \$5,000 in value,” as set forth in (i), then the statute limits the civil remedy to economic damages. 18 U.S.C. § 1030(g).

has not established that the computers at issue were “protected” within the contemplation of the statute. Second, the Defendant argues that the Plaintiff has failed to establish that the Defendant intentionally caused “damage” to the Plaintiff’s computers. Specifically, the Defendant argues that a person cannot simultaneously seek to damage a computer and gather passwords from the computer, because a person cannot recover passwords from a non-functioning computer.

The Plaintiff alleges that he and his employees used the computers at issue in connection with his law firm business. The Plaintiff also claims that the computers were connected to the internet. As a result, the complaint satisfies the statutory requirement that the computers must at least be “used in interstate ... commerce or communication” in order to be considered “protected.” 18 U.S.C. § 1030(e)(2)(B). In addition, the statute does not, as the Defendant suggests, apply only in the instance that a person intends to render a computer completely inoperable. Rather, the statute defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). The Plaintiff alleges that his computers presented “error messages, slow processing, and other indicators of technical problems.” Compl. ¶ 6. Error messages and slow processing constitute impairments to the integrity or availability of data. Therefore, assuming that all of the Plaintiff’s allegations are true, it is reasonable to infer that the Defendant may have intended to cause such limited damage to the computers at issue, even if she did not intend to render them completely inoperable. Accordingly, the Court finds that the Plaintiff has stated a valid claim under the Computer Fraud and Abuse Act.

#### **D. The Louisiana Electronic Surveillance Act**

The Louisiana Electronic Surveillance Act makes it unlawful for any person to

“[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire or oral communication.” LA. REV. STAT. ANN. § 15:1303(A)(1). Because the Louisiana Electronic Surveillance Act is modeled after the Federal Wiretap Act, “federal law is instructive in the areas where the provisional language coincides.” *Keller v. Aymond*, 98-844, p. 6 (La. App. 3 Cir. 12/23/98); 722 So. 2d 1224, 1227. Federal law, however, may not be instructive where the language differs. Importantly, the Louisiana Electronic Surveillance Act, unlike the Federal Wiretap Act, prohibits only the interception of “wire or oral communications”—it does not address the interception of “electronic communications.” LA. REV. STAT. ANN. § 15:1303(A)(1). The Louisiana Legislature included the term “electronic communications” in the statute several times—and even defined it—but did not expressly prohibit the interception of such communications in all circumstances. *See, e.g.*, LA. REV. STAT. ANN. § 15:1302(7)(a) (defining “electronic communication”). Rather, the Legislature expressly limited the scope of the statutory prohibition to the interception of “oral or wire” communications. LA. REV. STAT. ANN. § 15:1303(A)(1).

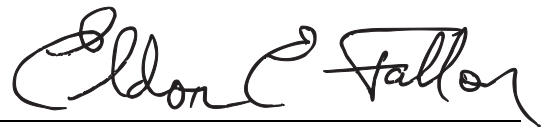
In the instant case, the Plaintiff does not allege that the Defendant intercepted oral or wire communications. The Plaintiff alleges only that the Defendant transmitted a computer virus that “works by gathering the passwords from the compromised computer and sending them to a remote computer by email or other means.” Compl. ¶ 9. Although the Plaintiff asserts that Louisiana courts interpret the Louisiana Electronic Surveillance Act to apply to electronic communications, the Plaintiff has not provided—and the Court has not identified—a single case supporting the Plaintiff’s invitation to disregard the plain, express language of the Act. Accordingly, the Court finds that the Plaintiff has failed to state a claim under the Louisiana Electronic Surveillance Act and, as a result, the Defendant’s motion to dismiss is granted as to

that claim.

#### IV. CONCLUSION

For the reasons listed above, the Defendant's Motion to Dismiss is GRANTED IN PART AND DENIED IN PART.

New Orleans, Louisiana, this 24th day of September, 2008.

A handwritten signature in cursive script, reading "Eldon C. Fallon". The signature is written in black ink and is positioned above a horizontal line.

UNITED STATES DISTRICT JUDGE