In the

United States Court of Appeals

For the Seventh Circuit

No. 15-1830

FIDLAR TECHNOLOGIES,

Plaintiff-Appellant,

v.

LPS REAL ESTATE DATA SOLUTIONS, INC.,

Defendant-Appellee.

Appeal from the United States District Court for the
Central District of Illinois.
No. 4:13-CV-4021 — **Sara Darrow**, *Judge*.

ARGUED NOVEMBER 5, 2015 — DECIDED JANUARY 21, 2016

Before FLAUM, MANION, and ROVNER, *Circuit Judges*.

FLAUM, *Circuit Judge*. Fidlar Technologies ("Fidlar") brings this action against LPS Real Estate Data Solutions, Inc. ("LPS") for violations of the Computer Fraud and Abuse Act ("CFAA") and the Illinois Computer Crime Prevention Law ("CCPL"). Fidlar claims that LPS improperly downloaded county land records provided through Fidlar's services. The district court granted summary judgment in favor of LPS. It

held that Fidlar failed to show that LPS acted with intent to defraud under CFAA § 1030(a)(4) or that LPS caused "damage" under § 1030(a)(5)(A). The court also rejected Fidlar's argument that LPS knew or had reason to know that it might cause loss as required by the CCPL. For the following reasons, we affirm.

I. Background

Fidlar is a technology company that develops software for county offices to manage public land records. Fidlar's software allows counties to digitize and index land records. Fidlar licenses its software to the counties, and the individual counties contract with users who want access to these land records.

One of Fidlar's software products, Laredo, provides users with remote internet access to county records. The "Laredo system," as Fidlar describes it, consists of three components: the county databases, the "Laredo client" (or just "the client"), and the "middle tier." The county databases store county land records and index data. The "Laredo client" is a user-interface that allows users to remotely access these land records and related data. Finally, the "middle tier" facilitates the communication between the Laredo client and a specific county database. Fidlar offers its county customers the option of whether to host the county database and middle tier components on the county's own servers or on Fidlar's servers. The client is stored on the user's own computer.

In order to use the client, a user must accept Fidlar's End-User License Agreement ("EULA"). In relevant part, the EULA provides that a user may "use … any portion of the software for any purpose," but it also provides that a user

may "not … copy the software covered by this Agreement in any manner." Importantly, the EULA specifies that it does not grant access to any county information. The authority to grant access to records remains with the relevant county.

When a user inputs a record search into the Laredo client, the client sends a request to the middle tier via the internet. The middle tier then retrieves the appropriate record from the county database and "streams" this record to the user through the Laredo client. In other words, the user can view an image of the record in the client, but cannot download or save it for later viewing. However, the client gives the user an option to "print" an image of the record, either on paper or to a PDF file.

The client communicates with the middle tier through a technology called Simple Object Access Protocol ("SOAP calls"). The Laredo client sends SOAP calls unencrypted over the internet. In order to access a particular record, the client generates the appropriate SOAP call and sends it to the middle tier. After analyzing the SOAP call, the middle tier retrieves the matching record and sends it back to the client for viewing. Each Laredo user has a unique username and password for each county with which it has an agreement. Accordingly, each SOAP call is coded with a corresponding unique identifier.

Fidlar tracks access to county records in order to facilitate billing by the individual counties. Each county develops its own subscription plan for access to its records. All the subscription plans charge a monthly fee set by the county based on time spent accessing records. Some—but not all—counties also charge a separate "print fee" (or "copy fee") for each record a user prints using the client. Fidlar also uses

SOAP calls to track access and printing. For example, if a user prints a record from the client, the client generates and sends a SOAP call of the print request to the middle tier where it is logged for billing purposes.

LPS is a real estate data analytics company that used Laredo to gather real property data. LPS's business requires a continuous acquisition of land records and data. It currently has agreements for access to public land records with approximately 2,600 counties nationwide. However, LPS is not interested in the land records themselves, but rather the data in these records.

To further its data collection efforts, in 2010, LPS contracted with 82 of Fidlar's county customers to gain access to their land records. For each of these 82 counties, LPS agreed to pay the monthly fee for unlimited access to the county's records. For those counties that charged separate print fees, LPS's unlimited subscription did not include printing—if LPS printed a record from the client, it was still charged the applicable print fee. Fidlar was not a party to any of the contracts between LPS and the individual counties.

In 2011, LPS designed a "web-harvester," a computer program to download county records en masse. To create the web-harvester, LPS ran a number of standard record searches and used a "traffic analyzer" to view the SOAP calls sent from the client to the middle tier. LPS then identified the SOAP calls necessary to retrieve records and developed its own client, the web-harvester, to emulate those SOAP calls and send them to the middle tier. [1] LPS's web-harvester only

[1] "Web-harvester" is in fact a misnomer since LPS's client retrieved records from the county databases, not the World Wide Web.

sent the SOAP calls necessary to retrieve records; it did not send other SOAP calls, such as those that track a user's activity. But every SOAP call did include LPS's unique identifier assigned by each county.

Like the Laredo client, the web-harvester allowed LPS to search for and retrieve any record from the county databases it subscribed to. However, LPS's web-harvester had three major differences from Fidlar's Laredo client. First, the web-harvester allowed LPS to acquire records en masse rather than viewing or printing them one at a time. Second, the web-harvester allowed LPS to download or save records, an option not available in the Laredo client. Third, LPS's web-harvester did not send any tracking data at all and did not register any print fees, even if LPS downloaded or saved a record.

LPS used its web-harvester to obtain a large number of records from the 82 county databases it subscribed to over approximately two years. It downloaded the records in bulk onto its computers and then sent the records to India. There, select data from the records were "keyed," or entered, into LPS's database. Throughout this period, LPS continued to pay for unlimited subscriptions in all 82 counties but did not incur (or pay) print fees for all of the records it acquired through its web-harvester. Indeed, essentially none of LPS's activities were tracked during this period. Nonetheless, LPS's web-harvester did not disrupt Fidlar's services to other users or alter any content in the middle tier or county databases.

In 2012, Fidlar received a message from one of its county customers noting that LPS was paying subscription fees but was not logging any time used. In early 2013, Fidlar decided

to investigate LPS. Based on server logs, Fidlar concluded that LPS was using a web-harvester instead of the Laredo client to obtain records.

On March 11, 2013, Fidlar filed this action in the Central District of Illinois alleging violations of the Computer Fraud and Abuse Act and the Illinois Computer Crime Prevention Law, as well as trespass to chattels. LPS moved to dismiss, filed a counterclaim, and requested a TRO and preliminary injunction to prevent Fidlar from reporting LPS's activities to the counties and from upgrading Laredo to prevent web-harvesting. The district court denied LPS's motion to dismiss and its requests for injunctive relief. On December 1, 2014, LPS moved for summary judgment on all of Fidlar's claims. On March 5, 2015, the district court granted LPS's motion for summary judgment and dismissed LPS's counterclaim as moot. Fidlar appeals.

II. Discussion

We review a district court's grant of summary judgment de novo. *Bunn v. Khoury Enters., Inc.*, 753 F.3d 676, 681 (7th Cir. 2014). Summary judgment is appropriate if there is no genuine dispute of material fact and the nonmoving party is entitled to judgment as a matter of law. *Id.* A "material fact" is one that affects the outcome of the suit. *Id.* A "genuine issue" exists as to any material fact when "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* at 681–82. In determining whether a genuine dispute of material fact exists, we view the record in the light most favorable to the nonmoving party, drawing reasonable inferences in the nonmovant's favor. *Id.* at 682.

A. Computer Fraud and Abuse Act Claim

The CFAA, 18 U.S.C. § 1030, is primarily a criminal anti-hacking statute. However, § 1030(g) provides a civil remedy for any person who suffers damage or loss due to a violation of § 1030. § 1030(g). The district court held that Fidlar failed to demonstrate a violation of § 1030. On appeal, Fidlar argues that LPS violated § 1030(a)(4) and § 1030(a)(5)(A). We review each of these arguments in turn.

1. Intent to Defraud Under § 1030(a)(4)

Section 1030(a)(4) punishes anyone who:

> [K]nowingly and *with intent to defraud*, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value ….

The district court held that no reasonable jury could find that LPS acted with intent to defraud. Fidlar maintains that LPS's use of its web-harvester constituted an intentional scheme to avoid paying print fees, thus defrauding the counties.

Although this Court has not previously examined this element of § 1030, we have explained that in similar statutes "intent to defraud means that the defendant acted willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for himself or causing financial loss to another." *United States v. Pust*, 798 F.3d 597, 600 (7th Cir. 2015) (quoting *United States v. Paneras*, 222 F.3d 406, 410 (7th Cir. 2000)) (internal quotation marks omitted). Because direct evidence of intent is often unavailable, intent to defraud "may be established by circumstantial evidence

and by inferences drawn from examining the scheme itself which demonstrate that the scheme was reasonably calculated to deceive persons of ordinary prudence and comprehension." *Id.* at 600–01.

Additionally, the legislative history of § 1030(a)(4) indicates that Congress intended for this provision to reach cases of computer theft. S. Rep. No. 99-432, at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486–87 ("The new subsection 1030(a)(4) to be created by this bill is designed to penalize thefts of property via computer that occur as part of a scheme to defraud."). The intent to defraud element is meant to distinguish computer theft from mere trespass. *Id.* at 10 ("[T]here must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable in the first instance as a misdemeanor. The element in the new paragraph (a)(4), requiring a showing of an intent to defraud, is meant to preserve that distinction ….").

We note at the outset that this is not a case of theft. It is undisputed that LPS had authority to access the county records as a general matter, the question is whether the *way* in which it did so violated the statute.

Nonetheless, appealing to the broad nature of § 1030(a)(4)'s language, Fidlar argues that LPS's conduct supports an inference of an intent to defraud. By using its web-harvester, LPS obtained county records at no additional cost. Moreover, LPS knew that printing records through the client resulted in an additional fee in some counties. And LPS received invoices that did not reflect any downloads it made using its web-harvester, suggesting that LPS was aware that Fidlar and the counties were not tracking its activities. Assuming that LPS otherwise would have paid a

print fee for the records it downloaded, LPS's web-harvester allowed it to avoid paying these fees. Therefore, Fidlar contends that LPS's "scheme" appears consistent with an intent to defraud.

By contrast, LPS argues that its conduct is consistent with a legitimate, non-fraudulent intent. By using its web-harvester, LPS rapidly acquired records en masse, something it could not do with the Laredo client, even if it paid print fees. In other words, LPS could have been driven by a need to access documents more quickly, and not by an intent to defraud the counties by avoiding print fees. Indeed, if LPS just wanted to avoid print fees, it could have done so through simpler means such as copying the salient data by hand, taking pictures of the records on its computer screens with a digital camera, or simply keying the data directly from the Laredo client. Hence, LPS contends that its intent was to engage in efficient and legitimate business practices, not to "deceive or cheat" the counties. *Pust*, 798 F.3d at 600.

Examining the "scheme" itself, we conclude that no reasonable juror could infer that LPS had an intent to defraud. In other words, LPS's conduct was not "reasonably calculated to deceive persons of ordinary prudence and comprehension." *Id.* at 601. First, LPS used its web-harvester even in those counties that did not charge a print fee. If LPS's intent was to evade print fees, it would have only used its web-harvester in counties that did charge print fees. The fact that LPS used its web-harvester in all counties suggests that its goal was to accelerate its data acquisition efforts. Second, LPS continued to pay for unlimited subscriptions in all 82 counties, even though it was not logging any time by using its web-harvester. If LPS intended to defraud the counties, it

could have selected a limited subscription for less money. Third, LPS did not conceal its use of a web-harvester.[2] In fact, each of LPS's SOAP requests contained its unique identifier. As a result, no reasonable jury could conclude that LPS had the requisite intent to defraud based only on the scheme itself.

Moreover, Fidlar failed to present sufficient circumstantial evidence from which a reasonable jury could conclude that LPS intended to commit fraud, or even that LPS knew its actions were fraudulent. LPS maintains that it honestly believed that its conduct was permissible under the county agreements. Fidlar cannot demonstrate that LPS intended to commit fraud without evidence that LPS knew that its conduct was fraudulent. *See id.* at 601 (considering whether the defendant knew "the fraudulent nature of the scheme" in assessing intent to defraud).

---

[2] Fidlar argues that LPS did conceal its conduct because LPS's web-harvester did not send SOAP calls that track user activity. But this conduct is entirely consistent with LPS's purported non-fraudulent reason for using a web-harvester in the first place. LPS designed its web-harvester to obtain records and a tracking function like the one built into Laredo was irrelevant to accomplishing that purpose.

Typically, a person who is concealing fraudulent activity will take unusual, out of the ordinary steps to do so. For example, in *United States v. Westerfield*, we considered the fact that a criminal defendant had directed fraudulent proceeds to a third party as evidence of concealment when "a seller rarely—if ever—directs 100% of the proceeds to a third party." 714 F.3d 480, 485–86 (7th Cir. 2013). In this case, LPS did not go out of its way to conceal its conduct. Rather, it merely designed a web-harvester in the simplest way it knew how. In fact, an LPS employee expressed skepticism as to whether LPS even could have ascertained how Fidlar tracked user activity.

None of the circumstantial evidence, including the testimony of LPS employees, the agreements governing LPS's access to county records, and the Laredo technology itself, undermines LPS's claim that it believed it could permissibly download records through its web-harvester without paying print fees. First, LPS presented testimony from its employees indicating that they believed that although printing a record resulted in a fee, downloading a record did not. For example, LPS's former Senior Vice President Erick Marroquin stated that he believed that LPS was "entitled to download images from the Laredo program without incurring a print charge." LPS also offered evidence that it did not use a web-harvester to avoid print fees. The employee who oversaw development of the web-harvester, John McCabe, testified that in designing the web-harvester, "no part of [the process] was to avoid a print fee" and that the purpose was "[e]fficiency, speed."[3]

[3] In a declaration supporting LPS's request for a temporary restraining order, McCabe stated that "many counties engage Fidlar Technologies to act as the exclusive provider of internet access to the county's public records" and that "[a]nyone interested in reviewing the public records online must download Fidlar's Laredo software and obtain a username and password from the county." These statements do not support a finding of intent to defraud. Taking the second statement first, it is undisputed that in order to gain access to these records, initially, LPS had to download the Laredo client and obtain a username and password from each county. But as McCabe's complete declaration illustrates, LPS's conduct did not stop there. Our inquiry is focused on what happened after—when LPS created and used its web-harvester. As for the first statement, it is also undisputed that the counties contracted exclusively with Fidlar to provide internet access to their records. But LPS did access the records through Fidlar. LPS's web-harvester connected through the middle tier to the county databases, both of which were

Fidlar's own conduct, moreover, bolsters LPS's testimony on this point. LPS presented evidence that Fidlar knew that at least two of LPS's competitors used third party programs to acquire record data via Laredo. In particular, CoreLogic used a "screen-scraper" to collect data from county records. Similarly, the First American Title Company used its own web-harvester to acquire records. Fidlar was aware of this conduct yet did not do anything to stop it. Indeed, in an internal e-mail, a Fidlar employee stated that Fidlar *could* make screen-scraping or web-harvesting illegal with a "simple disclaimer that states the information can't be scraped from the image." Taken together, this evidence suggests that even Fidlar itself did not believe that web-harvesting was impermissible.

Second, the agreements between LPS and the counties did not prohibit LPS from using a web-harvester or require LPS to access the records through the Laredo client. *Cf. EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003) ("[T]he public website provider can easily spell out explicitly what is forbidden …. If [the plaintiff] wants to ban [certain conduct], let it say so on the webpage or a link clearly marked as containing restrictions."). These agreements also did not prohibit LPS from downloading records or require LPS to pay a print fee for any records it downloaded.[4] Yet,

---

maintained by Fidlar, and did not access the county records directly. The question therefore is whether the Laredo client was the exclusive means of accessing county records, not whether Fidlar was the exclusive provider of remote access.

[4] Some of the county agreements and invoices stated that there was an additional fee for making "copies." But evidence presented by LPS indicates that it understood "copy" fees as synonymous with "print" fees and that neither a print fee nor a copy fee applied to downloads.

LPS derived its authority to access records entirely from these agreements. The agreement between LPS and Fidlar, the Laredo client EULA, stated that it does not grant access to any county information. So the EULA, by its own terms, did not limit—or even affect—LPS's access to county records.

Third, the Laredo client's technological limitations do not support an inference that LPS knew it could not download records. Fidlar contends that because the client was designed to prevent downloading records, LPS should have known that it was not authorized to do so.[5] But the client's technological limitations only show that LPS knew that it could not download records *through the Laredo client*. We see no reason why LPS should have inferred that it could not download records through a completely different program that it designed. LPS's access to records was tied to the individual agreements with each county—agreements that did not require LPS to use the Laredo client and that Fidlar was not even party to. Further, the EULA, which was the only agreement between Fidlar and LPS, expressly provided that it did not grant access to records and that access could only be granted by the relevant county. In other words, if LPS believed that the county agreements granted it the authority to access records through its own software, the limitations on

[5] The client did not give the user the option to download records and it disabled certain standard computer function such as the copy-paste and the print-screen functions. It also inhibited third party software from taking screen shots. Fidlar presented evidence that it hobbled the client intentionally as a way to generate revenue for the counties from print fees.

the Laredo client would seem to have no bearing on the permissible uses of that software.

Additionally, other characteristics of Fidlar's services suggested that downloading records through another program, like a web-harvester, was permissible. The middle tier did not impose any limitations on LPS's use of a web-harvester. Fidlar did not encrypt SOAP calls between the middle tier and the Laredo client. And the middle tier was accessible by means other than the Laredo client, including other Fidlar software products, such as Fidlar's Tapestry platform, as well as third-party applications. So while the option to download records was limited on the front-end by the client user-interface, it was completely open on the back-end by the middle tier's use of unsecured SOAP calls.

Fidlar attempts to cast doubt on LPS's claim that it did not intend to defraud the counties. First, Fidlar argues that the county invoices, which did not indicate any of LPS's web-harvester activity, support an inference that LPS intended to defraud the counties. Even assuming that LPS knew its activities were not being tracked as a result of these invoices, the invoices do not undermine LPS's contention that it believed its conduct was permissible. LPS's access was governed by the county agreements and the invoices did not give LPS cause to change its understanding of these agreements. The fact that LPS was not being billed for downloading records would only reinforce LPS's belief that its conduct was permissible under its unlimited subscriptions. Similarly, the fact that the counties continued to accept LPS's unlimited subscription fees (and that Fidlar continued to provide LPS access) without any inquiry into the company's minimal activity might have further reinforced LPS's understanding of

its arrangement. As a result, the invoices do not make an intent to defraud any more likely.

Second, Fidlar cites the testimony of Lynda Taylor. Taylor was a Senior Vice President at LPS until June 2010, prior to LPS's creation and use of its web-harvester. Taylor explained that during her tenure at LPS, her plan was to "pay selectively," "on an as-needed basis … because Laredo charged for time to be on the system and to look at the document images online, and then you paid extra if you wanted to actually get a copy of an image." She also stated that Laredo did not allow a user to "take control of the digital image" of a record. Fidlar argues that this testimony shows that LPS knew it could either view a record in the client or pay to print a record from the client, but could not download or "take control" of a record.

However, Fidlar misreads Taylor's testimony. Taylor was only referring to the limitations of the Laredo client. She did not testify that LPS was prohibited from downloading records using a web-harvester or through other means. In fact, Taylor's tenure predates LPS's creation and use of the web-harvester. And individuals employed at LPS at that time consistently testified that they believed LPS's conduct to be permissible.

Third, Fidlar points to testimony from Michael Hall, LPS's Director of Data Acquisition, who stated that a hypothetical fee of $0.50 or more per page to print a record would have been "cost prohibitive" for LPS. This hypothetical fee is the same as the actual print fee charged by some of the 82 counties. Accordingly, Fidlar argues that Hall's testimony supports an inference that LPS was defrauding the counties of this fee.

But Fidlar's argument largely misses the mark. Undoubtedly, Hall's testimony shows that LPS had much to gain if it wanted to avoid print fees. But this is obvious; LPS does not dispute that acquiring records via a web-harvester was far less expensive than printing them via the Laredo client. The problem with Fidlar's argument is the fact that printing records via the client was more expensive, or even economically infeasible for LPS, does not demonstrate that LPS intentionally avoided this expense. Hall's testimony is entirely consistent with LPS's narrative that it was not trying to avoid print fees. Rather, the fees were simply inconsequential to LPS's data acquisition efforts. Hence, Hall's testimony does not support an inference of an intent to defraud.

In sum, Fidlar attempts to convert its failure to prohibit LPS's action by contract into an allegation of criminal conduct. Despite its extensive efforts to paint LPS's conduct as fraudulent in nature, Fidlar has not pointed to any evidence that would allow a reasonable jury to find that LPS believed its conduct was fraudulent. Hence, we agree with the district court that no reasonable jury could conclude—based on this evidence alone—that LPS acted with an intent to defraud.

2. Damage Under § 1030(a)(5)(A)

Next, Fidlar contends that LPS violated § 1030(a)(5)(A), which punishes anyone who:

> [K]nowingly 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 ….

The district court held that LPS did not violate this provision because it found that LPS did not cause any damage under the statute.

Under the CFAA, "damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information …." § 1030(e)(8). Hence, "causes damage" encompasses clearly destructive behavior such as using a virus or worm or deleting data. *See, e.g., Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006). But it may also include less obviously invasive conduct, such as flooding an email account. *See, e.g., Pulte Homes, Inc. v. Laborers' Int'l Union*, 648 F.3d 295, 301–02 (6th Cir. 2011).

Fidlar claims that LPS caused damage to a protected computer—the middle tier servers—by "stopp[ing] the flow of information, causing a diminution in the completeness or availability of data." However, Fidlar admits that LPS did not alter any data or disrupt Fidlar's services in any way. LPS just avoided Fidlar's method of tracking user activity by not sending the necessary SOAP calls.

This interruption is not "damage" as defined by the statute. LPS's web-harvester did not impair the integrity or availability of Fidlar's data or systems; it simply downloaded the data requested without leaving a trace. Put another way, the middle tier servers, including the logs, were unaltered after LPS used its web-harvester.

Fidlar attempts to liken this case to *United States v. Mitra*, 405 F.3d 492 (7th Cir. 2005), but the two are readily distinguishable. In *Mitra*, this Court held that a defendant caused damage by blocking emergency radio communications. 405 F.3d at 494. Unlike in this case, the defendant in *Mitra* actual-

ly impaired the availability and integrity of a protected computer. His conduct prevented others from communicating through the public communication system. *See id.* at 493 (noting that the defendant's conduct "prevented the computer from receiving, on the control channel, data essential to parcel traffic among the other 19 channels" and that "[w]hen disturbances erupted, public safety departments were unable to coordinate their activities because the radio system was down"). By contrast, LPS did not prevent anyone from using the middle tier and county database servers nor did it alter any of the content on the servers.

Fidlar tries to sidestep this distinction by arguing that LPS caused damage to the entire "Laredo system" because it prevented the tracking component from functioning as Fidlar intended. But the statute only protects against damage "to a protected computer," including to systems on such a computer. §§ 1030(a)(5)(A); 1030(e)(8). The Laredo system is not a "computer," but rather a description of Fidlar's multitier architecture. *See* § 1030(e)(1) (defining "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device"). Hence, LPS cannot be liable for damaging the entire "Laredo system" under this statute.

In reality, Fidlar's claim is trespassory in nature. LPS accessed the middle tier servers without following Fidlar's "rules" (i.e., logging its activity or using the Laredo client). But by using the word "damage," and in light of the statutory definition, Congress intended this provision reach actual disruptions in service, not mere access, even if trespassory. *See Citrin*, 440 F.3d at 420 ("Congress was concerned with both … attacks by virus and worm writers, … and attacks by

disgruntled programmers who decide to trash the employer's data system on the way out …."); *cf.* § 1030(a)(2) (prohibiting unauthorized access to obtain information from a protected computer *without* requiring damage). Therefore, the district court was correct that no reasonable jury could conclude that LPS caused any damage within the meaning of the statute.

B. Illinois Computer Crime Prevention Law Claim

Like the CFAA, the Illinois CCPL is a criminal statute with a civil suit provision. Section 720 ILCS § 5/17-51(c) provides that "[w]hoever suffers loss by reason of a violation of subdivision (a)(4) of this Section may, in a civil action against the violator, obtain appropriate relief." Fidlar claims that LPS violated subdivision (a)(4)(C), which provides that:

> (a) A person commits computer tampering when he or she knowingly and without the authorization of a computer's owner or in excess of the authority granted to him or her: … (4) Inserts or attempts to insert a program into a computer or computer program *knowing or having reason to know that such program contains information or commands that will or may*: … (C) *cause loss* to the users of that computer or the users of a computer which accesses or which is accessed by such program ….

720 ILCS § 5/17-51(a)(4)(C) (emphasis added). The district court held that LPS had no reason to know that its use of a web-harvester would or might cause loss under the statute. The court reasoned that LPS never believed that the counties

were entitled to print fees for its use of a web-harvester, and thus there was no loss to the counties that LPS knew or should have known it was causing.

In support of its position that LPS violated the CCPL, Fidlar incorporates the same argument it made under CFAA § 1030(a)(4): LPS intentionally defrauded, and consequently intended to cause loss to, the counties. Indeed, under Illinois law, Fidlar can establish knowledge by demonstrating that LPS acted intentionally. *See* 720 ILCS § 5/4-5 ("When the law provides that acting knowingly suffices to establish an element of an offense, that element also is established if a person acts intentionally.").

But as discussed above, Fidlar cannot show that LPS intended to defraud the counties. LPS demonstrated that its intent was to efficiently acquire records in a way it believed to be permissible under the governing agreements. Its intent was not to avoid print fees. Accordingly, LPS did not intend to cause loss to the counties.[6]

For the same reason, Fidlar cannot show that LPS knew or had reason to know that it might cause loss to the counties. LPS was aware that some counties imposed print fees and that the counties obtained revenue from these fees. But given that LPS believed that it was entitled to download records without incurring a fee, it follows that LPS did not know or have reason to know that it was causing a loss. The fact that LPS could have paid print fees but chose not to does not establish a loss to the counties because LPS was not

[6] We note that the term "loss" in this provision is not defined by the CCPL nor by Illinois case law. But we agree with the district court that no matter what definition applies, the result is the same.

printing records. At a minimum, Fidlar must demonstrate that LPS had reason to know that the counties were entitled to the print fees they allegedly lost. However, from LPS's perspective, the counties were not entitled to anything beyond the unlimited subscription fees LPS was already paying. Therefore, we agree with the district court that no reasonable jury could conclude that LPS knew or had reason to know that it would or might cause a loss.

III. Conclusion

For the foregoing reasons, we AFFIRM the judgment of the district court.