In the

United States Court of Appeals

For the Seventh Circuit

No. 19-1936

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

EDWARD SOYBEL,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 17 CR 796 — **Matthew F. Kennelly**, *Judge.*

ARGUED JUNE 3, 2020 — DECIDED SEPTEMBER 8, 2021

Before SYKES, *Chief Judge*, and BAUER and ST. EVE, *Circuit Judges*.

SYKES, *Chief Judge*. Industrial-supply company W.W. Grainger was the victim of a series of cyberattacks against its computer systems in 2016. Grainger isolated the source of the intrusions to a single internet protocol ("IP")

address, which came from a high-rise apartment building where disgruntled former employee Edward Soybel lived.[1]

Grainger reported the attacks to the FBI. To confirm the source, the government sought and received a court order under the Pen Register Act, 18 U.S.C. §§ 3121 *et seq.*, authorizing the installation of pen registers and "trap and trace" devices to monitor internet traffic in and out of the building generally and Soybel's unit specifically.[2] Among the data collected, the pen registers recorded the IP addresses of the websites visited by internet users within Soybel's apartment. The IP pen registers were instrumental in confirming that Soybel unlawfully accessed Grainger's system. The district court denied Soybel's motion to suppress the pen-register evidence and its fruits, and a jury convicted him of 12 counts of violating the Computer Fraud and Abuse Act.

This appeal presents a constitutional issue of first impression for our circuit: whether the use of a pen register to identify IP addresses visited by a criminal suspect is a Fourth Amendment "search" that requires a warrant. We hold that it is not. IP pen registers are analogous in all material respects to the telephone pen registers that the Supreme Court upheld against a Fourth Amendment chal-

---

[1] Every device connected to the internet has a unique IP address, typically consisting of a sequence of numbers. *See United States v. Caira*, 833 F.3d 803, 805 (7th Cir. 2016). An IP address "is used to route information between devices, for example, between two computers." *United States v. Ulbricht*, 858 F.3d 71, 84 (2d Cir. 2017) (quotation marks omitted).

[2] A pen register records certain outgoing electronic signals, whereas a trap-and-trace device records incoming ones. *See* 18 U.S.C. § 3127(3)–(4). For the sake of simplicity, we use the term "pen register" to refer to both devices.

lenge in *Smith v. Maryland*, 442 U.S. 735 (1979). The connection between Soybel's IP address and external IP addresses was routed through a third party—here, an internet-service provider. Soybel has no expectation of privacy in the captured routing information, any more than the numbers he might dial from a landline telephone.

Soybel insists that this case is governed not by *Smith* but by *Carpenter v. United States*, 138 S. Ct. 2206 (2018). We disagree. *Carpenter* concerned historical cell-site location information ("CSLI"). The warrantless acquisition of that type of data implicates unique privacy interests that are absent here. Historical CSLI provides a detailed record of a person's past movements, which is made possible so long as he carries a cell phone. In contrast, the IP pen register had no ability to track Soybel's past movements. And *Carpenter* is also distinguishable based on the extent to which a person voluntarily conveys IP-address information to third parties. Accordingly, though our reasoning differs from the district judge's, we hold that the suppression motion was properly denied.

Soybel also challenges the sufficiency of the evidence on one of the 12 counts. We reject this argument and affirm the judgment in all respects.

I. Background

Edward Soybel worked as an IT contractor for Grainger's KeepStock business unit from November 2014 until he was fired in February 2016. KeepStock provides Grainger customers with proprietary software and industrial equipment-dispensing machines to optimize their inventory management. Dispensing machines at customer sites across the

country connect to computer servers at Grainger's Niles, Illinois facility, which also serves as the home base for the KeepStock IT helpdesk where Soybel worked.

KeepStock stores information about its dispensing machines and its customers' log-in credentials in large "database tables." Helpdesk staff have their own KeepStock usernames and passwords, and when logged in to the KeepStock system, they could add and delete information in the tables. Performing the same functions remotely (outside the Grainger firewall) required access to the KeepStock "desktop client"—an application downloaded to a computer.

In July 2016 Grainger discovered that over the course of a week, someone with Grainger log-in credentials had accessed KeepStock and deleted millions of records from the database tables. As a result, KeepStock was effectively shut down for Grainger employees and customers alike until IT personnel could restore the data. An internal investigation revealed that the culprit had deleted the records via the desktop client using the log-ins of several current KeepStock employees, including Soybel's former supervisor. Further investigation led Grainger to believe that the intrusions all came from the same IP address outside of Grainger's network. Grainger reported the IP address to the FBI, which then determined that the address came from a large apartment building in Chicago where Soybel lived with his mother.

However, the FBI could not yet confirm that Soybel was responsible. The identified IP address came not from an individual unit but from the building's "master router" that distributed internet service throughout the building. The

master router was, in effect, the middleman between the individual units and the rest of the internet. Each unit in the building had its own unique private IP address, but when an individual user accessed a website, only the master router's IP address would be visible to that website's servers. At the same time, the master router knew to which private IP address it should relay that website's traffic. The upshot is that when an internet user in the building connected to Grainger's servers, only the master router could confirm the private IP address—and thus the specific apartment unit—that was responsible for the KeepStock attacks.

To confirm its suspicions about Soybel, the government applied for an order under the Pen Register Act to install IP pen registers for the master router and Soybel's unit for 60 days. The data to be recorded was highly technical.[3] For our purposes it's enough to note that the government sought to collect (1) connections between the master router's and the unit's IP addresses on the one hand, and external IP addresses on the other; and (2) the time that the connections occurred. That is, the information from the pen registers would help the government determine whether and when Soybel tried to access KeepStock.

At the same time, the government's application specified that the pen registers would not record the *content* of any communications between IP addresses, an express limitation

[3] The pen registers could "record and decode dialing, routing, addressing, and signaling information (including IP addresses, [Media Access Control] addresses, port numbers, packet headers, and packet size) for all electronic communications transmitted to or from the [target IP addresses], and [could] record the date, time, and duration of such transmissions."

in the Pen Register Act. *See* 18 U.S.C. §§ 3121(c), 3127(3)–(4). The data the government would collect might show, for instance, that an internet user connected to a Google IP address.[4] But it could not reveal the specific Google website accessed (i.e., YouTube or Gmail), let alone what the user was doing within that website.

A district judge granted the application in September 2016. The order was not based on a finding of probable cause. Instead, as required by the Act, the judge found that the government had included the requisite certification that the information to be obtained was "relevant to an ongoing criminal investigation" into computer crimes. *Id.* § 3122(b)(2) (including the certification among the required contents for a Pen/Trap application); *id.* § 3123(a)(1) (specifying this finding as a prerequisite for the order).

The building's internet-service provider then installed the pen registers in the building's mechanical room without entering Soybel's unit. While the master router's pen register captured only internet connections to and from KeepStock's IP addresses, Soybel's pen register recorded all internet connections that came from that unit. Put differently, the pen register associated with his apartment recorded connections between his private IP address and the IP addresses of those websites that internet users in the apartment had visited. The pen registers revealed that Soybel's private IP address—and only Soybel's private IP address—attempted to connect to KeepStock 790 times between September and November

[4] The IP addresses for some servers are publicly available. Some websites permit users to input a given IP address and obtain certain identifying information about its source, much like a virtual phonebook.

2016. Grainger confirmed that these attempts came at the same time that the master router's IP address tried to breach the KeepStock firewall.

One of the recorded intrusions is particularly relevant for this appeal. In September 2016 Soybel changed the KeepStock password for Grainger business analyst Dan Hoehne in the middle of the night. Soybel clicked on a forgotten password option for Hoehne's username and used his own Gmail account as the recovery email. He then changed Hoehne's password to "1234" and temporarily locked Hoehne out of KeepStock. Though by this time Grainger had blocked the master router's IP address from accessing its system, forensic examination of Soybel's laptop later showed that he was able to change Hoehne's password using the IP address of a nearby apartment building.

A grand jury charged Soybel with 12 counts of violating the Computer Fraud and Abuse Act. *See* 18 U.S.C. § 1030. Count 10 related to the act of changing Hoehne's password and alleged that Soybel knowingly caused "the transmission of a program, information, code, or command" to "intentionally cause[] damage without authorization[] to a protected computer." *Id.* § 1030(a)(5)(A).

Following Soybel's indictment, the Supreme Court issued its decision in *Carpenter*, holding that the government must generally obtain a search warrant to access historical CSLI. 138 S. Ct. at 2220. The Court concluded that a court order under the Stored Communications Act is insufficient because it requires less than probable cause. *Id.* Soybel moved to suppress all evidence obtained as a result of the Pen/Trap order, arguing that *Carpenter* had broader Fourth Amendment implications beyond the CSLI context.

The judge denied the suppression motion. Though the judge was skeptical that *Carpenter* has any effect on pen registers, he declined to decide whether their use violates the Fourth Amendment. He instead denied Soybel's motion based on the good-faith exception to the exclusionary rule. The judge held that suppression was inappropriate because the officers relied in good faith on a pre-*Carpenter* understanding of the Pen Register Act in seeking the order. In other words, regardless of whether the Pen/Trap order violated Soybel's Fourth Amendment right to be free from unreasonable searches, the judge concluded that a reasonable officer could believe that compliance with the Act's requirements was sufficient for a lawful order.

Data obtained from the pen registers was front and center at Soybel's trial. The government also presented forensic evidence from Soybel's laptop, which showed—among other things—that Soybel had downloaded the KeepStock desktop client each time before he accessed the KeepStock system. As to Count 10, testimony showed that Hoehne was unable to access KeepStock until his password could be reset. And in closing argument the government emphasized that as a result of the breach, Hoehne could not provide necessary customer service.

A jury convicted Soybel on all 12 counts and further found that the offenses caused either a loss to Grainger during a one-year period aggregating at least $5,000 or damage affecting ten or more protected computers during a one-year period. The judge denied Soybel's motions for a judgment of acquittal and for a new trial, and Soybel appealed.

II. Discussion

Soybel contends that the use of the pen registers violated his Fourth Amendment right to be free from unreasonable searches. He also argues that insufficient evidence supported his conviction under Count 10.

A. Fourth Amendment Challenge

Soybel first argues that based on *Carpenter*, the judge should have excluded the IP pen-register evidence. We review this issue de novo, *see United States v. Mojica*, 863 F.3d 727, 731 (7th Cir. 2017), and conclude that the judge properly denied the suppression motion. Though the good-faith exception barred suppression here, we affirm because there was no Fourth Amendment violation in the first place. *See United States v. Reaves*, 796 F.3d 738, 741–42 (7th Cir. 2015) (explaining that we may affirm the denial of a motion to suppress "on any ground supported in the record").

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. To conduct a "search" under the Fourth Amendment, an officer generally must obtain a warrant supported by probable cause. *See Katz v. United States*, 389 U.S. 347, 359 (1967). But not all investigative actions are "searches" subject to Fourth Amendment scrutiny. Under the privacy-based framework relevant here, a "Fourth Amendment search does *not* occur … unless the individual manifested a subjective expectation of privacy in

the object of the challenged search[] and society [is] willing to recognize that expectation as reasonable."[5] *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (quotation marks omitted) (alteration in original).

The government installed the pen registers not based on a finding of probable cause but rather under a court order supported by a lesser showing of relevance as provided in the Pen Register Act. *See* §§ 3122(b)(2), 3123(a)(1). Soybel argues that the Fourth Amendment demands more. The government, on the other hand, maintains that the Fourth Amendment provides no protection because the pen registers did not entail a "search."

This issue turns on the application of the third-party doctrine. A core principle of *Katz* is that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. at 351. A person generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties," subjective expectations notwithstanding. *Smith*, 442 U.S. at 743–44 (collecting cases); *see also United States v. Miller*, 425 U.S. 435, 442 (1976) (finding no "legitimate expectation of privacy concerning the information kept in bank records" that a person "voluntarily convey[s] to [a] bank[] and expose[s] to [his] employees in the ordinary course of business"). Where the third-party doctrine applies, "the [g]overnment is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2216.

---

[5] Soybel does not suggest that the pen register intruded on any property-based interests.

Smith is the foundational case for the use of pen registers. At the request of the police, a telephone company installed a pen register at its central office that recorded outgoing phone numbers dialed on the defendant's landline phone. *Smith*, 442 U.S. at 745–46. The defendant moved to suppress the pen-register evidence because officers had not obtained a search warrant prior to the installation. *Id.* at 737. The Supreme Court held that no warrant was necessary because the officers had not conducted a Fourth Amendment search. *Id.* at 745–46. Critically, the pen register had only "limited capabilities," capturing the numbers dialed but not the identity of the caller, any sound, or even whether the call had been completed. *Id.* at 741–42. The case was thus distinguishable from *Katz*, where officers overheard the *substance* of the conversation via a listening device attached to a phone booth. 389 U.S. at 349–50.

The dialed phone numbers in *Smith* fit squarely within the emerging third-party doctrine. When a subscriber placed a call, the phone company's "switching equipment" routed the call and the phone company could make a permanent record of the number a subscriber dialed. 442 U.S. at 742. The Court noted that Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business" and thus "assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744. So Smith had no reasonable expectation of privacy "in the phone numbers he dialed" even though he dialed them from his home. *Id.* at 745–46.

The IP pen registers in this investigation are a new breed of pen registers compared to the one at issue in *Smith*. When

Soybel's IP address contacted Grainger's IP addresses (by way of the third-party internet-service provider and the master router), the pen registers recorded the fact and time of the connections. But technological differences don't necessarily beget constitutional ones. Before *Carpenter* the Second Circuit considered the use of an IP pen register under the Pen Register Act and held that under the logic of *Smith*, no search warrant is necessary. *See United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017) ("The recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in *Smith*."). And more generally, the circuits to have considered the question pre-*Carpenter* were in accord that the third-party doctrine extends to an individual's own IP address or the IP addresses of the websites he visits. *See, e.g.*, *id.* (destination IP addresses); *United States v. Wheelock*, 772 F.3d 825, 829 (8th Cir. 2014) (own IP address); *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (own IP address); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (destination IP addresses).

Soybel responds that *Carpenter* changed the Fourth Amendment calculus. *Carpenter* refined the third-party doctrine for a specific type of digital data: historical location information as revealed by CSLI. *See* 138 S. Ct. at 2211–12 (explaining that "[e]ach time [a] phone connects to a cell site, it generates a time-stamped record" stored by a wireless carrier). The officers in *Carpenter* obtained historical CSLI based on an order under the Stored Communications Act. Similar to the Pen Register Act, an order under the Stored Communications Act may be issued based on less than

probable cause; the government need only "offer[] specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The Court held that this lesser showing is not enough; the officers had "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements" by obtaining historical CSLI without a warrant supported by probable cause. *Carpenter*, 138 S. Ct. at 2219.

Soybel contends that after *Carpenter* he has a reasonable expectation of privacy in his "personal [i]nternet traffic data." We disagree. As three of our sister circuits have recognized, *Carpenter* has no bearing on the government's collection of IP-address data from a suspect's internet traffic. *See United States v. Trader*, 981 F.3d 961, 967–69 (11th Cir. 2020); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018). For starters, the Court in *Carpenter* stressed that its decision was a "narrow one." 138 S. Ct. at 2220. *Carpenter* thus was not a wholesale repudiation of *Smith* or the third-party doctrine generally. To the contrary, the Court emphasized that it did not "disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools." *Id.* Instead, the Court merely "decline[d] to extend *Smith* and *Miller* to cover the[] novel circumstances" presented by historical CSLI. *Id.* at 2217.

On this point *Carpenter* was "novel" both as to the instrumentality of the search and in the information captured. Given the extent to which people "compulsively carry cell phones with them all the time," a cell phone has become "almost a feature of human anatomy." *Id.* at 2218 (quotation

marks omitted). And because a cell phone "faithfully follows its owner" wherever he goes, the location information "provides an all-encompassing record of the holder's whereabouts," including his entry into "private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2217–18. When the phone is powered on, the result is "near perfect surveillance." *Id.* at 2218.

The Court explained that the privacy concern is magnified by the data's "retrospective quality" because historical CSLI gives "police access to a category of information otherwise unknowable." *Id.* Obtaining historical CSLI without a warrant would allow the government to effectively "travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers." *Id.* The "detailed chronicle of a person's physical presence compiled every day, every moment, over several years," the Court held, "implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 2220.

The unique features of historical CSLI are absent for IP-address data. The pen register was stationary and could not capture the whole of Soybel's physical movements. *Cf. Hood*, 920 F.3d at 92 (explaining that whereas CSLI captures the approximate "location of the cell phone user who generates that data simply by possessing the phone," IP-address data "is merely a string of numbers associated with a device that had, at one time, accessed a wireless network"). As was true in *Smith*, a recorded connection at most incidentally revealed when Soybel may have been in his apartment. But even that's not a given because the data was impersonal. A recording of "the existence of connections between communications devices" shows only that *someone* in Soybel's unit

was using the internet. *Ulbricht*, 858 F.3d at 97. It could not reveal the identity of the user—whether it be Soybel, his mother, or an unidentified guest. *Cf. Carpenter*, 138 S. Ct. at 2219 (noting that the "telephone call logs [in *Smith*] reveal little in the way of 'identifying information'"). The same cannot be said for CSLI, unless the cell phone's owner takes the unusual step of giving it to someone else.

Moreover, routing information obtained via a pen register isn't retrospective. The government could not effectively "travel back in time" by using an IP pen register. A pen register is only forward-looking; its usefulness extends only so far as it is installed and no further. And here, the government would have had to seek a renewal of the 60-day order if it needed data beyond that point. CSLI, in contrast, is continuously collected and available for the government's ready use so long as the cell carrier retains the records, which could be up to five years. *Id.* at 2218 (noting that a suspect would be "effectively … tailed every moment of every day for five years").

Perhaps recognizing that the IP-address information did not reveal much about his physical movements, Soybel contends that it provided an unwanted glimpse into his *mind*. He notes that the pen registers captured visits to Credit Karma and Match.com, so he argues that the pen register might provide an "intimate window" into his "familial, political, professional, religious, and sexual associations." *Id.* at 2217 (quotation marks omitted). But the same is true for telephone pen registers like the one the Court approved in *Smith*; by obtaining the numbers that a suspect dials, law enforcement could likewise determine whether he had called a bank, a political headquarters, a church, or a

romantic partner. And for each type of pen register, any intrusion on these interests is minimized by the fact that the government did not—and under the Pen Register Act, could not—intercept the content of the communications. *See* §§ 3121(c), 3127(3)–(4).

Differences in the data collected aside, *Carpenter* is also distinguishable on the extent to which Soybel assumed the risk by voluntarily communicating with third parties. The Court explained in *Carpenter* that CSLI "is not truly 'shared' as one normally understands the term" because "carrying [a cell phone] is indispensable to participation in modern society" and a cell-phone user opens himself up to tracking "without any affirmative act on the part of the user beyond powering up." 138 S. Ct. at 2220. We do not discount the importance of the internet in 2021. But it's not the case that Soybel created the data "without any affirmative act … beyond powering up." *Id.* An internet user creates connection data by "making the affirmative decision to access a website," just as the user of a landline generates a telephone-number record solely by choosing to dial it. *Hood*, 920 F.3d at 92 (explaining that "an [i]nternet user generates the IP address data … only by making the affirmative decision to access a website or application"). And here, Soybel took the affirmative step of *downloading* the desktop client and connecting to Grainger's servers remotely.

In short, this case bears the hallmarks of *Smith*, not *Carpenter*. And under *Smith* Soybel has no reasonable expectation of privacy in the routing information collected by the pen registers. Accordingly, we hold that an IP pen register is analogous in all material respects to a traditional telephone pen register. An IP address operates much like a phone

number, and "[l]ike telephone companies, internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible." *Ulbrecht*, 858 F.3d at 97. Though a person does not "dial" another's IP address in the ordinary sense, information was routed through a third party to complete the connection between the computer in Soybel's unit and the destination IP addresses. *See id.* at 96. In this respect, the master router—which directed internet traffic to and from Soybel's own IP address—is not unlike the telephone switchboard in *Smith*. And Soybel assumed the risk that by connecting to Grainger servers, the fact of the connection would be revealed to law enforcement. Soybel therefore has no reasonable expectation of privacy in this data.

Because the government did not conduct a Fourth Amendment search in this case, it need not have done more than obtain an order under the Pen Register Act. Even were we to hold to the contrary, suppression is unwarranted under the good-faith exception to the exclusionary rule. Under one variant of the good-faith exception, suppression is not the proper remedy for "evidence seized pursuant to a statute subsequently declared unconstitutional." *Illinois v. Krull*, 480 U.S. 340, 352–53. (1987). The "sole purpose" of the exclusionary rule, after all, "is to deter future Fourth Amendment violations." *Davis v. United States*, 564 U.S. 229, 236–37 (2011).

We have applied the *Krull* principle to permit the admission of CSLI evidence obtained based on a pre-*Carpenter* understanding of the Stored Communications Act. *See United States v. Curtis*, 901 F.3d 846, 849 (7th Cir. 2018). The same conclusion follows for a pre-*Carpenter* understanding

of the Pen Register Act, for which no court of appeals has suggested that the absence of probable cause is constitutionally suspect. "Penalizing [an] officer for the [legislature's alleged] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Krull*, 480 U.S. at 350 (quotation marks omitted). For this additional reason, suppression was properly denied.

B. Sufficiency of the Evidence for Count 10

Finally, Soybel contends that insufficient evidence supports his conviction for changing Hoehne's password. Count 10 charged Soybel with violating § 1030(a)(5)(A), which requires that the government prove that he "knowingly cause[d] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[d] damage without authorization[] to a protected computer." Soybel does not contest that he issued a command to change Hoehne's password. Nor does he challenge the special-verdict findings regarding the number of computers affected by the intrusion over a one-year period. He does dispute, however, that he caused "damage" when he changed Hoehne's password.

We review de novo the denial of a motion for judgment of acquittal and consider the evidence in the light most favorable to the jury's verdict. *United States v. Kelerchian*, 937 F.3d 895, 907 (7th Cir. 2019). We overturn a conviction only if the record contains no evidence from which a reasonable jury could determine guilt beyond a reasonable doubt. *United States v. Durham*, 645 F.3d 883, 892 (7th Cir. 2011).

Soybel has not overcome this high bar. Consistent with the statutory definition, the judge instructed the jury that

"damage" means "*any* impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (emphasis added). Soybel did not argue below, nor does he claim on appeal, that the judge should have done more to guide the jury.

Instructed this way, a reasonable jury could find that the password reset caused "damage" as the terms in the definition are ordinarily understood. To "impair" is to "damage or make worse … by diminishing in some material aspect." *Impair*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003). And to be "available" is to be "present or ready for immediate use." *Available*, *id.* The government presented evidence that the password reset locked Hoehne out of KeepStock and temporarily prevented him from servicing his customers. At the very least, a reasonable jury could find that Soybel's actions "impair[ed] … the … availability of … [the] system" by temporarily diminishing its readiness for Hoehne's immediate use.

Soybel counters that his actions caused no data loss and that KeepStock remained functional for other users. And he emphasizes that Grainger was able to quickly rectify the issue. Neither point is relevant under § 1030(e)(8). The broad definition of "damage" covers *any* impairment. It makes no difference that the problem was a quick fix on Grainger's end, nor does it matter that Soybel did not dismantle all or part of KeepStock more broadly. The evidence was sufficient to convict Soybel on Count 10.

AFFIRMED