No. _____

In The

Supreme Court of the United States

October Term, 2021

EDWARD SOYBEL,

Petitioner,

vs.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Seventh Circuit

PETITION FOR A WRIT OF CERTIORARI

Robert J. Palmer
Counsel of Record
rpalmer@maylorber.com
MAY • OBERFELL • LORBER
4100 Edison Lakes Parkway, Suite 100
Mishawaka, IN 46545
Rpalmer@maylorber.com
Phone: (574) 243-4100
Fax: (574) 232-9789

and

University of Notre Dame
School of Law
Notre Dame, IN 46556

Attorney for Petitioner

QUESTION PRESENTED

Whether the opinion of the Seventh Circuit Court of Appeals, deciding a constitutional issue of first impression for the Circuit, erroneously ruled that the use of a pen register to identify internet protocol (IP) addresses is not a Fourth Amendment "search" that requires a warrant.

PARTIES TO THE PROCEEDING

All parties to the proceeding are named in the caption.

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Page

Cases

Statutes

Other Authorities

Constitutional Provisions

Petitioner, Edward Soybel, respectfully requests that a Writ of Certiorari be issued to review the judgment of the United States Court of Appeals for the Seventh Circuit in this case.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Seventh Circuit is reported at *United States v. Soybel*, 13 F.4th 584 (7th Cir. 2021) (App. A). Judgment was entered on May 9, 2019. (App. B.)

STATEMENT OF JURISDICTION

The judgment of the United States Court of Appeals for the Seventh Circuit ("Court of Appeals") was entered on September 8, 2021. No petitions for rehearing were filed.

The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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."

STATEMENT OF THE CASE

The fundamental question in this case is whether the Seventh Circuit Court of Appeals erroneously decided a constitutional issue of first impression for the Circuit in determining that the use of a pen register to identify IP addresses is not a search under the Fourth Amendment.

A. Proceedings Below.

Edward Soybel was indicted on twelve counts of violating various provisions of the Computer Fraud and Abuse Act ("CFAA"). The first eleven counts allege

violations of 18 U.S.C. § 1030(a)(5)(A), which states that one may not "knowingly cause the transmission of a… command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer."

The Government applied for an order under the Pen Register Act to install IP pen registers for Soybel's apartment. The Government sought to collect: (1) connections between the master router and the apartment's IP addresses on the one hand, and external IP addresses on the other; and (2) the time that the connections occurred. The Government's application specified that the pen registers were not to record the content of any communications between IP addresses.

The district court granted the application in September 2016, not based on a finding of probable cause, but rather, based on the Government's certification that the information to be obtained was "relevant to an ongoing criminal investigation" into computer crimes.

After Soybel was indicted, this Court rendered its decision in *Carpenter v. United States*, 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018). Soybel moved to suppress all evidence obtained as a result of the District Court's Order, arguing that *Carpenter* required a finding of probable cause before authorizing installation of a pen register. The district court did not decide the Fourth Amendment issue, but rather, denied the motion to suppress based on the good faith exception to the exclusionary rule. The court ruled that suppression was inappropriate because the police officers relied in good faith on a pre-*Carpenter* understanding of the Pen Register Act in seeking the order.

A jury convicted Soybel on all twelve counts. Soybel was sentenced to a term of thirty-six months on each count to run concurrently. The court also ordered restitution in the sum of one hundred fourteen thousand fifty-six dollars.

Following the jury verdict, Soybel, on December 28, 2018 filed a motion for acquittal. The district court denied the motion on May 6, 2019. The district court entered judgment three days later.

Soybel filed a timely Notice of Appeal on May 15, 2019. The Seventh Circuit Court of Appeals affirmed the conviction on September 8, 2021.

B. Factual Background.

This Computer Fraud and Abuse Act ("CFAA") case focuses on an industrial supply company called W.W. Grainger ("Grainger"). Grainger provides a computer-based inventory management service called the "KeepStock" system. The KeepStock system helps customers manage their supply of Grainger products, as well as purchase additional goods from Grainger brand vending machines across the country. The KeepStock system is run off a number of Grainger servers in Niles, Illinois. One of those servers ("the database") contains company information, such as usernames and passwords for customers and KeepStock maintenance staff, commercial records for the operation and maintenance of Grainger's vending machines, and tables of Grainger's SEC audit history.

Numerous employees and contractors were responsible for maintaining the KeepStock system. For instance, Grainger gave KeepStock access to their database administration teams, their KeepStock support team, and their KeepStock help desk. These employees could log into KeepStock with a username and password,

and should they forget their password, they could ask KeepStock to perform a "password reset." A "password reset" tells the KeepStock system to send a new password, called a "recovery password," to an email address the user provides. Once these employees log in, dozens of them have the ability to view, add, or delete information and data in the KeepStock system. This includes the ability to view or alter KeepStock users' IDs and passwords. These individuals were referred to as either "Tier One" support staff, or support staff with "Administrative Access."

The Pen Register

In July 2016, Grainger detected an intrusion in the KeepStock system, which resulted in the deletion over a hundred thousand records. This prompted Grainger to open an internal security investigation, recruit a forensic investigation team, and notify FBI. It was eventually determined that much of the intruding traffic came from the public IP address 162.254.168.1 (hereinafter referred to as "IP 162"). A "public" IP address covers every unit within a building. So, if an individual living in an apartment complex connects to a website, such as Google, the Google computers would only see that the *public* IP address made the connection--not the individual unit. A router, on the other hand, distributes the internet connection to individual units. Every device in the building that connects to the internet receives a private IP address, located behind the router. The units' private IP addresses are not "broadcast" to the public internet like the building's public IP address—IP 162—would be.

An FBI agent working on the Grainger computer intrusion investigation reached out to Everywhere Wireless, the internet service provider issuing IP 162 to

customers, and obtained business records for IP 162. The records indicated that IP 162 was assigned to an apartment building located at 5030 North Marine Drive. In late August 2016, Grainger told the FBI agent that Edward Soybel, a former Grainger employee, lived at that address. The next step was to identify exactly which unit the unauthorized intrusions were coming from, which could be accomplished by using a pen register.

A pen register is "a device that law enforcement uses to try and record any time one device contacts or makes a connection with another device." Pen registers were historically used for phones--they had the capability of recording when one phone number would call another, and which phone numbers were connecting. With computers, pen registers record connections between two IP addresses. They record the date and time of the connection, along with the name of the connecting IP addresses. A pen register does not record content, but instead records the fact that a connection occurred. In the case of a public IP address—like IP 162, which covered an entire apartment complex—anyone residing at the physical address associated with that IP address would make a connection with the public IP address when using the internet.

Pursuant to 18 U.S.C. § 3121, law enforcement officials obtained a court order supported by a certification of "relevance" before installing a pen register for IP 162. The application for the court order simply stated that "[t]here is evidence that Subject IP Addresses have been and will be used in furtherance of a criminal offense, namely computer crime . . . and that information concerning the ongoing

use of the Subject IP Addresses will provide evidence of that offense." The application also noted that "the suspect(s) repeatedly used Subject IP Address 1 [IP 162] during the course of gaining unauthorized access to the victim company's computer networks and using that access to damage the networks" and that "[o]ne of the individuals under investigation, a former IT contractor for the victim company, appears to be the user of Subject IP Address 2, which accessed the internet through Subject IP Address 1." No additional evidence was provided in the application for the court order. Since IP 162 was a public address, this meant that any pen register for that IP address would capture the internet connections for anyone in that apartment complex, regardless of where they were located. At the time the pen register was installed, law enforcement officials "weren't sure that Mr. Soybel was involved . . . or not" and "[i]t wasn't apparent to anyone that he was responsible for [the Grainger] computer intrusions." Although they knew that Mr. Soybel resided at the physical address associated with IP 162, law enforcement officials were interested in monitoring internet traffic from *all* of the units to make sure there were no other units connecting to KeepStock. Regardless, law enforcement had a particular interest in monitoring internet traffic from unit 401, where Mr. Soybel resided. As such, the pen register was designed to capture two main forms of internet traffic: first, it captured all internet traffic coming from unit 401, and second, it captured internet traffic from all other units, but only traffic directed at the two KeepStock IP addresses.

After the pen register was installed, law enforcement officials determined that IP 162 connected to (or attempted to connect to) KeepStock IP addresses 790 times during September and October 2016. Everywhere Wireless determined that these attempted intrusions were coming from Mr. Soybel's unit.

REASONS FOR GRANTING THE WRIT

THE PETITION SHOULD BE GRANTED BECAUSE THE OPINION BELOW ERRONEOUSLY DECIDED A CONSTITUTIONAL ISSUE OF FIRST IMPRESSION FOR THE CIRCUIT IN RULING THAT THE USE OF A PEN REGISTER TO IDENTIFY IP ADDRESSES IS NOT A SEARCH PURSUANT TO THE FOURTH AMENDMENT WHICH REQUIRES A WARRANT.

I. The Pen Register Act Violates The Fourth Amendment Of The United States Constitution Because It Does Not Require A Warrant Supported By Probable Cause For A Government Agency To Install A Pen Register.

Under 18 U.S.C. § 3121, hereinafter referred to as the Pen Register Act, the use or installation of a pen register or trap and trace device is prohibited without first obtaining a court order. The court order application must be made by a Government attorney and need only certify "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [the requesting] agency." 18 U.S.C. § 3121(b)(2) (1986). Under the Pen Register Act, probable cause is not required for an authorized government agency to install a pen register. The only necessary criteria to obtain a pen register court order is a bare certification of "relevance" by the requesting government attorney.

The Fourth Amendment, however, provides that [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

searches and seizures, shall not be violated . . . but upon probable cause[.]" U.S. Const. Amend. IV. In *Carpenter v. United States*, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018), this Court held that the government's warrantless acquisition of a defendant's historical cell site location information ("CSLI") violated the Fourth Amendment, and that a court order obtained pursuant to the Stored Communications Act (18 U.S.C. § 2703(d)) was constitutionally insufficient. Here, the lower court erred in denying defendant's motion to suppress evidence because the internet traffic information obtained by a pen register is analogous to the cell site location information discussed in *Carpenter*. Thus, the Pen Register Act violates the Fourth Amendment since it only requires a court order supported by a minimal showing or relevance, while *Carpenter* requires a warrant supported by probable cause. The Seventh Circuit similarly erred in affirming the lower court's decision.

A. The "third party doctrine," historically applied to telephone pen registers, should not be indiscriminately applied to modern computer pen registers because computer pen registers capture a wide breadth of information that could not have been anticipated by the early telephone pen register cases.

Pen registers were historically used to capture telephone connections--they had the capability of recording when one phone number would call another, and which phone numbers were connecting. In *Smith v. Maryland*, 442 U.S. 735 (1979), this Court held that government officials could install pen registers to capture telephone numbers dialed by individuals without violating the Fourth Amendment because telephone users have "no legitimate expectation of privacy" because they

"voluntarily convey[] numerical information to the telephone company" and "assume[] the risk that the company would reveal to police the numbers . . . dialed." *Id.* at 744. Similarly, in *United States v. Miller*, 425 U.S. 435, the Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Id.* at 443.

While the "third-party doctrine" from *Smith* and *Miller* has long been applied to cases involving pen registers, this Court's subsequent decision in *Carpenter* challenged the idea that the third-party doctrine is a per se bar against Fourth Amendment protection. The Court held that *Carpenter* required the court to "apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of cell phone signals." *Id.* at 2216. Although the fact that an individual user "continuously reveals his location to his wireless carrier implicates the third-party doctrine of *Smith* and *Miller*," which involve telephone numbers and bank records, respectively, "it is not clear whether [the] logic [of the doctrine] extends to the qualitatively different category of cell-site records." *Id.* at 2216–17. The Court in *Carpenter* reasoned that cell-site records are "qualitatively different" from telephone numbers and bank records because cell phones are essentially an extension of the individual--they go "wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 2217. As a result, the

Court also concluded that "the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221.

This Court in *Carpenter* held that its decision was "a narrow one," and noted that *Smith* and *Miller* were still applicable to "conventional surveillance techniques and tools." However, the door was left open with regards to other "novel" forms of technological data. In fact, in *Riley v. California*, 573 U.S. 373 (2014), this Court held that "any extension" of analog era reasoning to "digital data has to rest on its own bottom." *Id.* at 393. The Court further explained that "an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records" that would "keep defendants and judges guessing for years to come." *Id.* at 401.

Although *Smith* and *Miller* have traditionally been applied to cases involving pen registers for landline telephones, *Carpenter* should be extended to cases involving the application of pen registers to IP addresses. Computer pen registers are not among those "conventional" surveillance techniques described in *Carpenter*, which include tools such as security cameras and "other business records that might incidentally reveal location information." *Id.* at 2210. Internet traffic information is nothing like the analog telephones of bygone eras—it is a modern phenomenon that captures a wide array of personal data that could not have been anticipated by the analog-era cases, and it requires a modern solution explaining when and how such information can be accessed by law enforcement.

B. The post-*Carpenter* analysis depends on whether an individual has a reasonable expectation of privacy in the information obtained by law enforcement officials, and individuals certainly have a reasonable expectation of privacy in their internet browsing data.

The post-*Carpenter* analysis is not whether a third party has access to an individual suspect's personal internet traffic data, but rather, whether an individual suspect has a reasonable expectation of privacy when it comes to their personal internet traffic data. In *Carpenter*, the Court held that data regarding an individual's movements provide "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 138 S. Ct. at 2217. The Court further held that an individual "maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," and such records are therefore protected under the Fourth Amendment. *Id.* Internet traffic information, like cell site location information, provides an "intimate window into a person's life" by revealing the websites an individual visits. In this case, the records show visits to websites such as Credit Karma and Match.com. Internet traffic data is nothing like the phone records discussed in *Smith*. The internet is a ubiquitous part of people's everyday lives in a way that landline telephones have never been. Google sees 3.5 billion searches every day—equating to 1.2 trillion searches per year.[1] Eighty-one percent of adults in the United States report that they use the

[1] Smart Insights, Search Engine Statistics 2018 (Jan. 30, 2018), available at https://www.smartinsights.com/search -engine-marketing/search-engine-statistics/.

internet either "several times a day" or "almost constantly."[2] People use the internet to conduct business, plan vacations, manage finances, and find love--and, according to a 2014 survey, 70 percent of respondents consider the websites they visit to be "very sensitive" or "somewhat sensitive."[3]

In *Smith*, the pen register applied to the defendant's telephone had "limited capabilities"—it disclosed "only the telephone numbers that have been dialed," and could not reveal "any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed." *Smith*, 442 U.S. at 741. In this case, on the other hand, the pen register allowed the government to identify both the source and destination IP addresses, along with their physical location and names. While the pen registers purport to not reveal "content"—i.e., the body of an email or the words typed into a search engine will not be transmitted—IP addresses can be considered "content" in themselves in that they provide "an intimate window into a person's life" by revealing "his 'familial, political, professional, religious, and sexual associations,'" like the cell site location information in *Carpenter*. *Carpenter*, 138 S. Ct. at 2217. If cell phones are considered an extension of an individual's physical self, internet traffic data should be considered an extension of an individual's mind.

---

[2] Pew Research Center, About Three-in-Ten U.S. Adults Say They are 'Almost Constantly' Online (July 25, 2019), available at https://www.pewresearch.org/fact-tank/2019/07/25/americans-going-online-almost-constantly/.

[3] Pew Research Center, Public Perceptions of Privacy and Security in the Post-Snowden Era (Nov. 12, 2014), available at http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/11/PI_PublicPerceptionsofPrivacy_ 111214.pdf.

Furthermore, Everywhere Wireless maintained an express privacy policy stating: "The privacy and security of your information is a foremost consideration of Everywhere Wireless. We only collect information that is necessary to service our relationship with you and the services to which you subscribe; *nothing more*." The policy also states: "We do not and will not track or monitor your online browsing activity." Any reasonable customer reading this policy would interpret it to mean that their internet browsing data would be kept private—or, at the very least, not invaded without probable cause and a search warrant. Thus, individuals have a reasonable expectation of privacy in their internet traffic data, and such data is entitled to Fourth Amendment protection.

C. Under *Carpenter*, law enforcement officials should be required to demonstrate probable cause before obtaining permission to install a pen register for an IP address, and here, the court order application lacked probable cause.

This Court in *Carpenter* held that a warrant supported by probable cause "is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party." *Carpenter*, 138 S. Ct. at 2222. After determining that individuals had a reasonable expectation of privacy in their cell site location information, the Court also concluded that "the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221.

In *Carpenter*, the government acted in accordance with 18 U.S.C. § 2703(d), the Stored Communications Act, when it obtained a court order (instead of a warrant) to access the defendant's historical cell phone records. *Id.* at 2212. The Stored Communications Act did not require a showing of probable cause—it simply

required the government to offer "specific and articulable facts showing that there are reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation." *Id.* Since the "relevancy" requirement of the Stored Communications Act was deemed "a 'gigantic' departure from the probable cause rule," the Court determined that "an order issued under § 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records." *Id.* at 2221.

The Pen Register Act is even more egregious than the Stored Communications Act: the Stored Communications Act at least required the government to provide "specific and articulable facts" demonstrating relevance before obtaining a court order, whereas the Pen Register Act merely requires a bare "certification by the applicant" that the information obtained is likely to be relevant. 18 U.S.C. § 3121(b)(2) (1986). In this case, the Government did not identify any specific evidence in its pen register application—it merely identified the suspect living at the address associated with IP 162 and noted that "[t]here is evidence that Subject IP Addresses have been and will be used in furtherance of a criminal offense, namely computer crime, . . . and that information concerning the ongoing use of the Subject IP Addresses will provide evidence of that offense." In fact, the court order was obtained the very same day the pen register application was filed.

Allowing the Government to access potentially sensitive internet browsing information without a warrant supported by probable cause is an unconstitutional breach of an individual's reasonable expectation of privacy. Here, the Government did not show probable cause in the court order application—instead, it only

provided a bare certification that the information sought would be "relevant" to an ongoing investigation. Therefore, evidence admitted in this case pursuant to 18 U.S.C. § 3121, the Pen Register Act, must be excluded since the Pen Register Act violates the Fourth Amendment of the United States Constitution by failing to require a warrant supported by probable cause.

CONCLUSION

For the foregoing reasons, petitioner, Edward Soybel, respectfully requests this Court to grant this petition for writ of certiorari.

Respectfully submitted,

Robert J. Palmer
Counsel of Record
rpalmer@maylorber.com
MAY • OBERFELL • LORBER
4100 Edison Lakes Parkway, Suite 100
Mishawaka, IN 46545
Phone: (574) 243-4100
Fax: (574) 232-9789
and
University of Notre Dame
School of Law
Notre Dame, IN 46556

Attorney for Petitioner

APPENDIX A

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

APPENDIX B

15

UNITED STATES DISTRICT COURT

Northern District of Illinois

UNITED STATES OF AMERICA
v.
EDWARD SOYBEL

JUDGMENT IN A CRIMINAL CASE

Case Number: 1:17-CR-00796(1)

USM Number: 52758-424

Vadim A. Glozman
Defendant's Attorney

THE DEFENDANT:

☐ pleaded guilty to count(s)

☐ pleaded nolo contendere to count(s) which was accepted by the court.

☒ was found guilty on counts one (1), two (2), three (3), four (4), five (5), six (6), seven (7), eight (8), nine (9), ten (10), eleven (11), and twelve (12) of the indictment after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section / Nature of Offense		Offense Ended	Count
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentinall cause damage to a computer	7/24/2016	1
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a	7/24/2016	2
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	3
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	4
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	5
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	6
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	7
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	8
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	9
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(c)(4)(B)(i)	Transmission of a command to intentionally cause damage to a computer	7/24/2016	10
18 U.S.C. § 1030(a)(5)(A), 18 U.S.C. § 1030(b) and 18 U.S.C. § 1030(c)(4)(B)(i) and (ii)	Attempted transmission of a command with the intent to cause damage to a computer	7/24/2016	11
18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 1030(b) and 18 U.S.C. § 1030(a)(2)(A),	Attempt to access a computer without authorization	7/24/2016	12

The defendant is sentenced as provided in pages 3 through 7 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

☐ The defendant has been found not guilty on count(s)

☐ Count(s) dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States Attorney for this District within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States Attorney of material changes in economic circumstances.

May 8, 2019
Date of Imposition of Judgment

Signature of Judge
Matthew F. Kennelly, United States District Judge

Name and Title of Judge

5-9-2019
Date

DEFENDANT: EDWARD SOYBEL
CASE NUMBER: 1:17-CR-00796(1)

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of:

Thirty-six (36) months as to counts one (1), two (2), three (3), four (4), five (5), six (6), seven (7), eight (8), nine (9), ten (10), eleven (11), and twelve (12) of the indictment, to run concurrently.

☒ The court makes the following recommendations to the Bureau of Prisons: The Court recommends the defendant be placed in an institution where defendant can participate in the residential drug program at an appropriate time during his incarceration. The Court recommends defendant be placed in either FPC Terre Haute or FPC Oxford because his only family lives in the Chicago area. Further, the Court directs that any costs of imprisonment be waived due to defendant's inability to pay.

☒ The defendant is remanded to the custody of the United States Marshal.

☐ The defendant shall surrender to the United States Marshal for this district:

- ☐ at on
- ☐ as notified by the United States Marshal.
- ☐ The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:
  - ☐ before 2:00 pm on
  - ☐ as notified by the United States Marshal.
  - ☐ as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows: _____

_____

_____

Defendant delivered on _____ to _____ at _____, with a certified copy of this judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

DEFENDANT: EDWARD SOYBEL
CASE NUMBER: 1:17-CR-00796(1)

MANDATORY CONDITIONS OF SUPERVISED RELEASE PURSUANT TO 18 U.S.C § 3583(d)

Upon release from imprisonment, you shall be on supervised release for a term of:

Three (3) years as to counts one (1), two (2), three (3), four (4), five (5), six (6), seven (7), eight (8), nine (9), ten (10), and eleven (11) of the indictment and one (1) year as to count twelve (12) of the indictment, to run concurrently.

You must report to the probation office in the district to which you are released within 72 hours of release from the custody of the Bureau of Prisons. The court imposes those conditions identified below:

During the period of supervised release:

1. The defendant shall not commit another Federal, State, or local crime.

2. The defendant shall not unlawfully possess a controlled substance.

3. The defendant shall cooperate in the collection of a DNA sample.

DISCRETIONARY CONDITIONS OF SUPERVISED RELEASE PURSUANT TO 18 U.S.C § 3563(b) AND 18 U.S.C § 3583(d)

Discretionary Conditions — The court orders that you abide by the following conditions during the term of supervised release because such conditions are reasonably related to the factors set forth in **§ 3553(a)(1)** and **(a)(2)(B), (C), and (D);** such conditions involve only such deprivations of liberty or property as are reasonably necessary for the purposes indicated in **§ 3553 (a)(2) (B), (C), and (D);** and such conditions are consistent with any pertinent policy statement issued by the Sentencing Commission pursuant to **28 U.S.C. 994a.**
The court imposes those conditions identified below:

During the period of supervised release:

1. The defendant shall not possess a firearm, ammunition, or a dangerous weapon.

2. The defendant shall report to the probation office in the federal judicial district to which the defendant is released within 72 hours of release from the custody of the Bureau of Prisons.

3. During the term of supervised release, the defendant shall report to the probation officer in a manner and frequency directed by the probation officer.

4. The defendant shall not knowingly leave the federal judicial district in which the defendant is being supervised without the permission of the court or probation officer.

5. The defendant shall permit a probation officer to visit the defendant at any reasonable time at home or any other reasonable location specified by the probation officer. The defendant shall permit confiscation of any contraband observed in plain view of the probation officer.

6. The defendant shall answer truthfully any inquiries by the probation officer, subject to any constitutional or other applicable privilege.

7. The defendant shall notify the probation officer within 72 hours after becoming aware of any change or planned change in the defendant's employer, workplace, or residence.

8. The defendant shall notify the probation officer within 72 hours after being arrested, charged with a crime, or questioned by a law enforcement officer.

9. The defendant shall refrain from excessive use of alcoholic beverages, defined as having a blood alcohol concentration of greater than 0.08%, and shall refrain from any use of a controlled substance, as defined in section 102 of the Controlled Substances Act, 21 U.S.C. § 802, without a prescription from a licensed medical practitioner.14.The defendant shall participate in a substance abuse treatment program and in a mental health treatment program. This condition may be satisfied by participation in a "dual diagnosis" (substance abuse and mental health) treatment program. The mental health program shall include a focus on anger management. The program shall be approved by the probation officer. The defendant shall abide by the rules and regulations of the program and shall

take any mental health medications that are prescribed by the defendant's treatment provider. The program may include testing, up to a maximum of 104 tests per year, to determine the defendant's compliance with the requirements of the program. The probation officer, in consultation with the treatment provider, shall supervise the defendant's participation in the program (provider, location, duration, intensity, etc.).

SPECIAL CONDITIONS OF SUPERVISED RELEASE PURSUANT TO 18 U.S.C. 3563(b)(22) and 3583(d)
The court imposes those conditions identified below:

During the term of supervised release:

1. The defendant shall not enter into any agreement to act as an informer or special agent of a law enforcement agency without the permission of the court.

2. If the defendant is not gainfully employed after the first 60 days of supervision, or for any 60 period during the term of supervision, the defendant shall perform 10 hours of community service per week at the direction of the probation officer until she is gainfully employed at lawful employment. The total amount of community service shall not exceed 200 hours over the term of supervision.

3. Any financial obligations imposed by the judgment in this case are due immediately. Any such obligations that remain unpaid when defendant's term of supervised release commences in an amount that is at least 15% of the defendant's net monthly income, defined as income net of reasonable expenses for basic necessities such as food, shelter, utilities, insurance, and employment-related expenses.

4. While any financial obligations imposed by the judgment are outstanding:

    a. The defendant shall apply all monies received from income tax refunds, lottery or gambling winnings, judgments, and/or any other unanticipated or unexpected financial gains to the outstanding court-ordered financial obligation.

    b. The defendant shall not incur new credit charges or open additional lines of credit without the approval of the probation officer.

    c. The defendant shall provide the probation officer with access to any requested financial information for use in connection with collection of outstanding restitution obligations.

    d. Within 72 hours of any significant change in the defendant's economic circumstances, the defendant must notify the probation officer about the change.

5. Any costs of supervised release are waived due to defendant's inability to pay.

DEFENDANT: EDWARD SOYBEL
CASE NUMBER: 1:17-CR-00796(1)

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	JVTA Assessment*	Fine	Restitution
TOTALS	$1,125.00	$.00	$.00	$ 114,056.00

☐ The determination of restitution is deferred until . An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.

☒ The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

W.W. Grainger, Inc.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to **18 U.S.C. § 3664(i)**, all nonfederal victims must be paid before the United States is paid.

☐ Restitution amount ordered pursuant to plea agreement $

☐ The defendant must pay interest on restitution and a fine of more than $2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant **to 18 U.S.C. § 3612(f)**. All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to **18 U.S.C. § 3612(g)**.

☒ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

- ☒ the interest requirement is waived for the restitution.
- ☐ the interest requirement for the is modified as follows:

☐ The defendant's non-exempt assets, if any, are subject to immediate execution to satisfy any outstanding restitution or fine obligations.

* Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.
* Findings for the total amount of losses are required under **Chapters 109A, 110, 110A, and 113A of Title 18** for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: EDWARD SOYBEL
CASE NUMBER: 1:17-CR-00796(1)

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A ☒ Lump sum payment of $115,181.00 due immediately.

☐ balance due not later than , or

☒ balance due in accordance with ☐ C, ☐ D, ☐ E, or ☒ F below; or

B ☐ Payment to begin immediately (may be combined with ☐ C, ☐ D, or ☐ F below); or

C ☐ Payment in equal *(e.g. weekly, monthly, quarterly)* installments of $ over a period of *(e.g., months or years)*, to commence *(e.g., 30 or 60 days)* after the date of this judgment; or

D ☐ Payment in equal *(e.g. weekly, monthly, quarterly)* installments of $ over a period of *(e.g., months or years)*, to commence *(e.g., 30 or 60 days)* after release from imprisonment to a term of supervision; or

E ☐ Payment during the term of supervised release will commence within *(e.g., 30 or 60 days)* after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or

F ☒ Special instructions regarding the payment of criminal monetary penalties:
Any financial obligations imposed by the judgment in this case are due immediately. Any such obligations that remain unpaid when defendant's term of supervised release commences in an amount that is at least 15% of the defendant's net monthly income, defined as income net of reasonable expenses for basic necessities such as food, shelter, utilities, insurance, and employment-related expenses. While any financial obligations imposed by the judgment are outstanding:

a. The defendant shall apply all monies received from income tax refunds, lottery or gambling winnings, judgments, and/or any other unanticipated or unexpected financial gains to the outstanding court-ordered financial obligation.
b. The defendant shall not incur new credit charges or open additional lines of credit without the approval of the probation officer.
c. The defendant shall provide the probation officer with access to any requested financial information for use in connection with collection of outstanding restitution obligations.
d. Within 72 hours of any significant change in the defendant's economic circumstances, the defendant must notify the probation officer about the change.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

☐ Joint and Several

Case Number **Defendant and Co-Defendant Names (including defendant number)**	**Total Amount**	**Joint and Several Amount**	**Corresponding Payee, if Appropriate**

See above for Defendant and Co-Defendant Names and Case Numbers (*including defendant number*), Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

☐ The defendant shall pay the cost of prosecution.
☐ The defendant shall pay the following court cost(s):
☐ The defendant shall forfeit the defendant's interest in the following property to the United States:

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) penalties, and (8) costs, including cost of prosecution and court costs.