No. 19-15114-BB

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

Jason Sartori,

Plaintiff-Appellant,

v.

Julie Schrodt,

Defendant-Appellee.

On Appeal from a Final Judgment of the
United States District Court for the Northern District of Florida
Case No. 3:18-cv-204-RV/HTC, Hon. Roger Vinson

BRIEF FOR APPELLEE JULIE SCHRODT

Hannah M. Beiderwieden
Student Counsel
Colin P. Shannon
Student Counsel

Brian Wolfman
GEORGETOWN LAW APPELLATE
COURTS IMMERSION CLINIC
600 New Jersey Ave., NW, Suite 312
Washington, D.C. 20001
(202) 661-6582
wolfmanb@georgetown.edu

Larry A. Matthews
Raymond F. Higgins, III
MATTHEWS & HIGGINS, LLC
114 East Gregory Street
Post Office Box 13145
Pensacola, FL 32591-3145
(850) 434-2200

Counsel for Defendant-Appellee Julie Schrodt

December 14, 2020

No. 19-15114-BB

Jason Sartori, Plaintiff-Appellant

v.

Julie Schrodt, Defendant-Appellee

CERTIFICATE OF INTERESTED PERSONS

Under this Court's Rule 26.1-1, Defendant-Appellee Julie Schrodt states that the following people and entities have an interest in the outcome of this appeal:

Beiderwieden, Hannah M.

Cannon, Hope T., U.S. Magistrate Judge

Georgetown Law Appellate Courts Immersion Clinic

Higgins, Raymond F., III

Kahn, Charles J., Jr., U.S. Magistrate Judge

Law Office of Michael Stanski

Matthews & Higgins, LLC

Matthews, Larry A.

Sartori, Jason

Schrodt, Julie

Shannon, Colin P.

Stanski, Michael

Vinson, Roger, U.S. District Judge

Wolfman, Brian

December 14, 2020

Respectfully submitted,

/s/Brian Wolfman
Brian Wolfman
GEORGETOWN LAW APPELLATE COURTS
IMMERSION CLINIC
600 New Jersey Ave., NW, Suite 312
Washington, D.C. 20001
(202) 661-6582
wolfmanb@georgetown.edu

Counsel for Defendant-Appellee Julie Schrodt

STATEMENT REGARDING ORAL ARGUMENT

Oral argument is not necessary. The issues presented are straightforward and were properly resolved by the district court in a comprehensive opinion. Oral argument would not, therefore, significantly aid the Court's resolution of this appeal.

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases **Page(s)**

TABLE OF CITATIONS—continued

Page(s)

TABLE OF CITATIONS—continued

Page(s)

TABLE OF CITATIONS—continued

Page(s)

Statutes

TABLE OF CITATIONS—continued

Page(s)

Other Authorities

ISSUES PRESENTED

The Computer Fraud and Abuse Act (CFAA) and the Stored Communications Act (SCA) are criminal laws aimed at deterring and punishing cyber hacking. Both establish civil remedies for the behavior they criminalize. The CFAA prohibits intentionally accessing information from a protected computer, but only when done without authorization. *See* 18 U.S.C. § 1030(a)(2)(C). In a civil CFAA suit, the plaintiff must also suffer losses of at least $5,000 because of the violation. *See id.* § 1030(g), (c)(4)(A)(i)(I).

The SCA prohibits unauthorized access to communications in electronic storage. *See* 18 U.S.C. § 2701(a). "Electronic storage" is "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17).

The district court rejected Plaintiff-Appellant Jason Sartori's claims that his then-wife, Defendant-Appellee Julie Schrodt, had violated the CFAA and the SCA by reading already-opened Skype and Gmail messages revealing Sartori's extramarital affairs.

The issues presented are:

I. Whether all of Sartori's claims fail because Schrodt was authorized to access the Skype and Gmail accounts under the CFAA and the SCA.

II. Alternatively, whether Sartori's CFAA claims also fail because Sartori has not satisfied the $5,000-loss requirement.

III. Alternatively, whether Sartori's SCA claims also fail because his messages were not in "electronic storage" under the Act given that he had already opened them.

STATEMENT OF THE CASE

Plaintiff-Appellant Jason Sartori is, as the district court put it, "a man suing his ex-wife for money damages while he is in prison for assaulting her" after she discovered his many extramarital affairs. Revised Appendix (App.) 200. Sartori maintains that Defendant-Appellee Julie Schrodt violated two federal criminal statutes that target cyber hacking by logging onto a shared computer, accessing a Skype account she had created, and twice accessing a Gmail account Sartori was still signed into. *Id.* at 199.

Sartori contends that Schrodt violated the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, when she accessed their shared computer and obtained evidence of his extramarital affairs from the Skype and Gmail accounts. He also asserts that she violated the Stored Communications Act (SCA), 18 U.S.C. § 2701, when she logged into the Skype account and opened the Gmail account, in both cases reading damning messages Sartori had already opened.

The district court granted summary judgment for Schrodt on all counts. It held that Sartori's use of the shared computer and the Skype account did not violate either statute because Schrodt's access was authorized: The computer was jointly held, marital property, and Schrodt herself created the Skype account with login credentials the couple used for other family accounts. And, as to Schrodt's initial access to the Gmail account, the court found no CFAA violation because Sartori failed to show any losses authorized by the Act and no SCA violation because the SCA doesn't prohibit access to emails that have already been delivered and opened. As for the later visit to the Gmail account, the court held that Sartori impliedly consented to Schrodt's access. This Court should affirm for these reasons and others discussed below.

I. Factual background

A. Schrodt managed the family household, including its shared digital accounts.

Julie Schrodt and Jason Sartori met as undergraduates at the University of Florida. App. 26 (¶ 1). They married in 2003. *Id.* Sartori later joined the United States Army and, by 2016, was stationed at Eglin Air Force Base, holding the rank of major. *See id.* at 88.

Schrodt was a stay-at-home mother to their three children. App. 27 (¶¶ 2-3). She managed the household, including taking primary responsibility for the children's schooling and extracurricular activities. *See id.* at 33-34 (¶¶ 8(c), (h), (k)). Sartori could not have advanced in the military without Schrodt's support. *See id.* at 28 (¶ 6(b)).

Schrodt also took a lead role setting up various online accounts using standard family usernames and passwords. *See* App. 84 (¶ 7). For example, Schrodt set up the Skype account at issue here using the family's usual login credentials to allow Sartori to communicate with the family while he was deployed. *Id.*; *see also id.* at 110 (¶ 6), 176.

When Sartori was away, Schrodt used a Sony computer to perform personal and family tasks. *See* App. 108-09. The family also had another, jointly owned personal computer, a Toshiba laptop, the use of which is at issue in this litigation. *See id.* at 84 (¶ 6). Sartori took that laptop with him on deployments but would use it for personal purposes exclusively; he used separate government systems for work. *See id.* at 84 (¶ 8), 176-77. When Sartori was at home, the laptop was typically kept in the couple's master bedroom, a spare room, or a similar place, "with the understanding [Schrodt] may need access" to it. *Id.* at 84 (¶ 8). At these times, Schrodt would use the laptop for everyday tasks like looking up directions or bank information, or to download files from the

internet. *Id.* at 174. Sartori testified that he never told Schrodt she could not use the laptop. *Id.* at 105.

B. Schrodt logs onto the jointly owned computer and discovers Sartori's many extramarital affairs.

On April 1, 2016, Sartori returned home from a three-month deployment. App. 84 (¶ 5). On April 5, Schrodt accessed the Toshiba laptop in the master bedroom and opened Skype with the login credentials that she had created for the account. *Id.* at 84 (¶¶ 6, 8). Schrodt "discovered multiple sexually explicit photographs and inappropriate conversations between [Sartori] and female contacts." *Id.* at 84 (¶ 9). Distraught at what she found, Schrodt sent one of the women a photo of her children and said, "Thanks to you, these three boys' lives as they know it is ruined." *Id.* at 157. She then printed all of the incriminating Skype messages. *Id.* at 85 (¶ 11).

While still on the computer, Schrodt opened an internet browser and "typed in Gmail.com." App. 151. Because his "account had never been logged out of," Sartori's Gmail inbox immediately "popped up," and Schrodt could see his emails. *Id.*; *see also id.* at 85 (¶ 12). Schrodt read many emails corroborating what the Skype messages showed: Sartori was having affairs with multiple women. *See id.* at 85-86 (¶¶ 10, 12, 17).

All the emails and Skype messages that Schrodt read had already been opened by Sartori. App. 85 (¶ 13). Schrodt did not print or download any emails on April 5. *See id.* at 85. About a month later, on May 6, Schrodt accessed Sartori's Gmail account a second time without having to enter a password. *See id.* at 85-86 (¶ 17). She then downloaded onto a thumb drive all of the emails demonstrating Sartori's extramarital relationships. *Id.*

All told, Sartori had affairs with at least six women. App. 88 (¶ 2); *see id.* at 92 (¶ 5a) (identifying nine women with whom Sartori had "inappropriate relationships"). Many of Sartori's relationships were with uniformed Army personnel. Sartori bragged to one of these women that he had slept with four service members while deployed in 2016. *Id.* at 93 (¶¶ 5a(2)-(4)). At least one relationship was with an enlisted staff sergeant in Sartori's Army Group, *id.* at 89 (¶ 3d), 97 (¶ 5e(1)), in violation of the Uniform Code of Military Justice's prohibition against sexual relationships between officers and enlisted personnel, *id.* at 97 (¶ 5e n.11).

C. Sartori lashes out as his marriage and career fall apart.

On April 6, Schrodt hired a divorce lawyer and gave him a copy of the Skype transcripts. App. 85 (¶ 14). The next day, Schrodt confronted Sartori, showed him copies of the Skype messages, and told him she was filing for divorce. *Id.* at 85 (¶ 15). Sartori did not subsequently change the account passwords because "[t]he cat [was] already out of the bag" and there was then "[n]othing to hide." *Id.* at 106-07 (Sartori Dep.).

Though Sartori was not concerned about Schrodt's future access to the online accounts, he was concerned that Schrodt's response to his betrayal would harm his career and finances. *See* App. 90 (¶ 4a n.4). Sartori's conduct became increasingly controlling and violent. He told Schrodt "[y]our friends connected to the military will kill my career which will affect you and [the] boys." *Id.* at 90 (¶ 4a n.4). On April 23, Sartori physically attacked and battered Schrodt. *See id.* at 121-22 (court-martial proceedings).

Sartori was arrested and faced criminal domestic-violence charges in state court based on allegations including that he "brandish[ed] a loaded weapon in front of his young son and strangl[ed] [Schrodt] while she held their infant in her arms." *See* App. 185 n.5; *see also id.* at 28-29, 35, 89 (¶ 3b n.2). Though these state-law charges were later dropped, Sartori was ordered by the military not to have "any physical or verbal contact" with Schrodt. *Id.* at 28-29, 96 (¶ 11c). Schrodt notified the military about the attack but did not at that time "provide any further details of her husband's infidelities." *Id.* at 89 (¶ 3b). Sartori, meanwhile, responded by twice attempting (unsuccessfully) to have Schrodt arrested. *Id.* at 29-30.

In August 2016, an Army sergeant informed Sartori's Group Commander that Sartori was having an affair with the Group Secretary. App. 88-89 (¶ 3a). Army personnel then reached out to and met with Schrodt. *See id.* at 86 (¶ 20), 89 (¶ 3b), 155, 184. The Army "requested any information that might assist in the case." *Id.* at 86 (¶ 20). After Schrodt turned over copies of the Skype and Gmail messages and accompanying pictures, *id.* at 86 (¶ 21), the Army started an administrative investigation, *see id.* at 89 (¶ 3c). Schrodt was subsequently interviewed by an Army investigator. *Id.* at 91 (¶ 4c).

The investigation concluded in January 2017. *See* App. 88. It found that Sartori had engaged in adultery and disobeyed his superior officer's order to have "no contact" with Schrodt in violation of the Uniform Code of Military Justice. *Id.* at 92-99. Sartori and Schrodt's divorce was finalized three months later. *See id.* at 45, 83. The next month, an Army board of inquiry recommended Sartori's dishonorable discharge from the military. *Id.* at 100-03, 185.

Less than a year later, Sartori filed this suit against Schrodt, as detailed below. *See* App. 7. Sartori has since been convicted in a military court-martial of multiple domestic-violence charges, including "assault consummated by a battery," and sentenced to ten years in prison. *Id.* at 121-22, 124. Because of his dishonorable discharge and subsequent court-martial, Sartori no longer receives an income with which to support Schrodt and the children. *See id.* at 166, 200.

II. Procedural background

A. Sartori sued Schrodt. App. 1. The amended complaint alleges violations of the CFAA, 18 U.S.C. § 1030, and the SCA, 18 U.S.C. § 2701. *Id.* at 20-23. Schrodt allegedly violated the CFAA by accessing the laptop itself, the Gmail account, and the Skype account, *id.* at 20-21, and the SCA by accessing both the Gmail and Skype accounts, *id.* at 22-23. Sartori sought declaratory and injunctive relief, damages, and attorney's fees and costs. *Id.* at 23.[1]

The CFAA requires Sartori to prove that Schrodt "(1) intentionally accessed a computer, (2) without authorization or in excess of her authorization, (3) obtained information thereon, and (4) caused him to suffer a loss of at least $5,000.00." D. Ct. Order, App. 189 (citing 18 U.S.C. § 1030(a)(2)(C), (c)(4)(A)(i)(I)). The SCA makes it unlawful to intentionally access without authorization "a facility through which an electronic communication service (ECS) is provided and to obtain access 'to a wire or electronic communication while it is in electronic storage.'" *Id.* at 192 (italics removed)

[1] Sartori also alleged state-law claims, which the district court dismissed. *See* App. 52. Sartori has abandoned those claims on appeal.

(quoting 18 U.S.C. § 2701(a)). "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* (italics removed) (quoting 18 U.S.C. § 2510(17)).

B. The district court denied Schrodt's motion to dismiss Sartori's CFAA and SCA claims, allowing the parties an opportunity to build a record. App. 49-50. After discovery, Schrodt moved for summary judgment. *Id.* at 61. As to the CFAA, Schrodt argued that she was authorized to access the laptop and the information contained in it because it was jointly held, marital property, foreclosing any violations under the Act. *Id.* at 71-72. She pointed out that she was authorized to access the Skype and Gmail accounts because she set up the Skype account and her authority extended to openly accessible information on the jointly held computer. *See id.* at 72, 76. She also argued that Sartori failed, even after discovery, to show that he suffered any losses, let alone the $5,000 in losses the CFAA requires. *Id.* at 72-75. As to the SCA, Schrodt argued that no violation occurred because she was authorized to access the messages and because the messages had already been read by Sartori, meaning they were neither held in "temporary, intermediate storage" pending delivery nor stored for "purposes of backup protection" as required for SCA liability. *Id.* at 76-77.

The district court agreed with Schrodt. App. 200. First, it found meritless Sartori's allegation that Schrodt violated the CFAA and the SCA by accessing the laptop and the Skype account. *Id.* at 185-86. She was authorized to access the laptop, the district court held, because it was jointly held, marital property, was kept in common areas of their

home, and was used by both parties. *Id.* at 185. And because Schrodt created the login credentials for the Skype account, using the same password the parties used for other family accounts, she was also authorized to access Skype. *Id.* at 185-86.

Second, the court concluded that Schrodt did not violate the CFAA or the SCA by accessing Sartori's Gmail account on April 5 and May 6. App. 191, 198. It first acknowledged that accessing a spouse's email account without authorization could violate the SCA and the CFAA but questioned whether doing so on a family computer, without having to enter a password, was prohibited by either statute. *Id.* at 187-88. Without deciding that question, the court held that Schrodt's May 6 Gmail access did not violate either statute because Schrodt had, at a minimum, implied authority to access the account given that Sartori never changed his password after Schrodt's earlier April 5 access. *Id.* at 186, 188. In support, the court noted that Sartori testified that he wasn't concerned about Schrodt having "any additional access or anything like that" because "the cat [was] already out of the bag." *Id.*

As for the earlier April 5 Gmail access, the court held that no CFAA violation occurred because Sartori hadn't shown $5,000 in losses resulting from Schrodt's access. App. 189-91. The costs associated with the divorce proceedings were not a direct result of Schrodt's Gmail access because she learned about the affairs from Skype, and Sartori had not shown that he incurred any costs by having to assess the damage from what he called Schrodt's "cyber strike." *Id.* at 190-91. As for the SCA, the court explained that opened emails are not in "electronic storage" because they are neither held in temporary storage pending delivery nor stored for "purposes of backup protection," entitling Schrodt to summary judgment. *Id.* at 193, 198.

SUMMARY OF ARGUMENT

I. All of Sartori's CFAA and SCA claims fail because Schrodt was authorized to access the Skype and Gmail accounts. As the district court recognized, Schrodt could not have lacked authorization to access Skype because she alone set up the account, using the same password Schrodt and Sartori used for other family accounts. If the account belonged to any one person, that person was Schrodt, not Sartori. In any case, Sartori never told Schrodt that she couldn't use the account or in any way limited her authorized access. Schrodt was also authorized to access the Gmail account via their shared computer on both dates because she was not required to enter a password and the account was readily accessible; Sartori never logged out of the account, so the emails just "popped up" when Schrodt typed in "Gmail.com." App. 151. And, as the district court correctly held, Schrodt had implied consent to access Gmail again in May because Sartori never changed his password or logged out of the account, despite knowing that Schrodt had accessed it in April. In fact, Sartori testified that he didn't care that Schrodt accessed the account again.

II. Sartori's CFAA claims fail for another, independent reason: He cannot show that Schrodt's conduct caused him $5,000 in losses as the statute requires. Sartori has not pointed to any record evidence to support his alleged losses, and his claims fail for that reason alone. But even if he had, Sartori's alleged losses—the costs of litigating this case and a separate divorce proceeding—do not constitute cognizable losses under the CFAA. The statute recognizes two distinct types of losses: consequential damages resulting from interruption of service, and the direct costs of responding to unauthorized computer access, like conducting a damage assessment and restoring data

lost as a result of that access. *See* 18 U.S.C. § 1030(e)(11). Because Schrodt's account access did not cause any service interruption, Sartori cannot recover consequential damages. And Sartori's alleged costs aren't covered by the second category of losses because they are wholly unrelated to the types of recoverable costs listed in the statute.

III. Sartori's SCA claims also fail for a separate, independent reason: The messages at issue were not in "electronic storage" when Schrodt read them, as the statute requires. Sartori had already opened all the Skype and Gmail messages, and "electronic storage" does not include opened messages held after delivery. As relevant here, "electronic storage" includes only storage (1) "by an electronic communication service" (2) "of such communication" (3) "for purposes of backup protection." *See* 18 U.S.C. § 2510(17)(B).

Each of these elements excludes opened messages. "Electronic communication services" include only sending and receiving communications and exclude permanent storage of opened and delivered messages. "Such communication" limits Section 2510(17)(B)'s scope to backup copies of communications defined in the preceding phrase—only those in "temporary, intermediate storage … incidental" to transmission. *See* 18 U.S.C. § 2510(17)(A). In other words, Section 2510(17)(B) applies only to backup copies of *unopened* messages. And the "purposes of backup protection" are limited under the SCA to backing up messages awaiting transmission, which, again, excludes already-opened messages.

ARGUMENT

Julie Schrodt did not violate the CFAA or the SCA. As explained in part I below, Schrodt was authorized to access both the Gmail and Skype accounts, dooming this appeal under both the CFAA and the SCA. Part II shows that Sartori's CFAA claims also fail because he has not met the CFAA's $5,000-loss requirement, and part III demonstrates that Sartori's SCA claims are meritless because opened messages are not held in "electronic storage" under the Act.

I. Schrodt did not violate the CFAA or the SCA because she was authorized to access the Skype and Gmail accounts.

A person violates the CFAA or the SCA only if she accesses "without authorization," or by "exceed[ing] authorized access," information from a protected computer, *see* 18 U.S.C. § 1030(a)(2)(C) (CFAA), or held in electronic storage, *see id.* § 2701(a) (SCA). "Authorization" has the same meaning under both statutes. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1002-03 (9th Cir. 2019).

The district court held that Schrodt was authorized to access the laptop itself because it was jointly held, marital property stored in common parts of the marital home, and Schrodt had used it on prior occasions. App. 185. That holding is not at issue here because Sartori has not challenged it before this Court. *See NLRB v. Allied Med. Transp., Inc.*, 805 F.3d 1000, 1009 (11th Cir. 2015).

The district court also held that Schrodt was authorized to access the Skype account, *see* App. 185-86, and Sartori's contrary argument, as explained below, should be rejected. Sartori has not pursued any argument on appeal that Schrodt lacked authorization to access Gmail on April 5 and makes only a cryptic reference to the district court's holding

that Schrodt had implied authorization to access Gmail on May 6. *See* Sartori Br. 20. He has therefore forfeited his claim that Schrodt's use of the Gmail account was unauthorized, *see Allied Med. Transp., Inc.*, 805 F.3d at 1009, and this Court should affirm as to Schrodt's Gmail access on that basis. In any case, as we now explain, Schrodt was authorized to access both Skype and Gmail.

A. Schrodt was authorized to access the Skype account.

The district court correctly held that Schrodt was authorized to access the Skype account because she alone set up the account, using the same password Schrodt and Sartori used for other family accounts. *See* App. 185-86.

1. Under the CFAA and the SCA, someone lacks authorization only when she doesn't have permission to access a computer or relevant facility, or when already-given permission has been explicitly revoked. *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016). As the Skype account-creator, *see* App. 84 (¶ 7), Schrodt could not have lacked authorization. That is, an individual "who use[s] his personal information to create the account and establish a password" is "clearly the person duly authorized" to access it. *Hoofnagle v. Smyth-Wythe Airport Comm'n*, No. 1:15-CV-00008, 2016 WL 3014702, at *11 (W.D. Va. May 24, 2016).

Sartori disagrees, arguing that Schrodt lacked authorization to access the Skype account because she never received his express permission to use it. Sartori Br. 26-27. That makes no sense. No decision of which we are aware embraces the strange concept that someone who creates a personal online account is somehow unauthorized to access it. *See Butler v. Enter. Integration Corp.*, 459 F. Supp. 3d 78, 105 (D.D.C. 2020) ("Plaintiffs

cite no cases supporting the proposition that a company cannot access its own email servers."). Indeed, as between Sartori and Schrodt, if any one person had authority to use the Skype account, that person would have been Schrodt, because she created the account. It would be *Sartori's* authority to use the account that would have to be inferred from the circumstances.

But Schrodt was authorized even if we assume that the account belonged to both Schrodt and Sartori. Courts have held that someone with password access cannot lack authorization (which, of course, Schrodt had here). For example, in *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 612, 620 (E.D. Pa. 2013), the defendants, departing company managers, were authorized to access their employer's computers because they "had user names and passwords" to the company's network. *See also Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1327-29, 1343 (N.D. Ga. 2007). Because Schrodt had the Skype password, it was irrelevant that she didn't generally use the account. *See* D. Ct. Order, App. 186 n.6.

Even assuming (counterfactually) that Sartori had superior ownership rights to the Skype account, Sartori would have had to expressly revoke Schrodt's authorization to render her Skype access unlawful, as occurred, for example, in *Power Ventures*, 844 F.3d at 1067. There, the defendant initially had authority to access Facebook's computers, but Facebook expressly revoked it by sending a cease-and-desist letter. *Id.* The record showed that the defendant knew it no longer had permission to access Facebook's computers and did so anyway by intentionally circumventing Facebook's software barriers. *Id.* Here, by contrast, Sartori never told Schrodt she couldn't use the Skype account, *see* App. 105; *see also id.* at 84 (¶ 7), 85 (¶ 16), 176, and it should go without

saying that Schrodt, who created the Skype login credentials in the first place, did not circumvent technological barriers to access the account.

2. Sartori also argues that Schrodt "exceeded [her] authorized access" to Skype, *see* 18 U.S.C. § 1030(a)(2), because she accessed the account in a "covert manner" with the intent to provide the messages to her divorce lawyer and to the Army. Sartori Br. 27-28. This argument fails from the start. Schrodt could not have known what she would find when she opened Skype, so she could not have formed the intent that Sartori ascribes to her. *See* App. 84 (¶ 9). (And, besides, she did not give that information to the Army until the Army asked for it months later. *Id.* at 86 (¶¶ 20-21), 89 (¶ 3b).)

In any case, even if we assume (again, counterfactually) that Schrodt had accessed the Skype account to gather information about the extramarital affairs, she still would not have exceeded her authorization. The SCA does not expressly define "exceeds authorized access," *see* 18 U.S.C. §§ 2510, 2711, but the CFAA defines it as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6). Thus, a person with permission to access a computer may violate these statutes if she accesses information for a purpose other than the one for which she was authorized. *See United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010).[2]

[2] Other circuits have taken a different approach, which looks not to an individual's purpose in accessing information but only to whether she accesses files or data that she was not permitted to obtain via an initial authorization. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 523-28 (2d Cir. 2015). The Supreme Court is currently considering this issue. *See United States v. Van Buren*, 940 F.3d 1192, 1207-08 (11th Cir. 2019) (refusing to overrule *Rodriguez*), *cert. granted*, 140 S. Ct. 2667 (Apr. 20, 2020). Schrodt was authorized to access the computer and Skype, and her authorization could not have

The key question on the facts here, then, is whether the scope of Schrodt's authorization was clearly communicated, *see Rodriguez*, 628 F.3d at 1263, not whether, as Sartori asserts, Schrodt had the "subjective intent" to exceed her authorized access, *see* Sartori Br. 28. That makes sense because a person cannot knowingly exceed her authorization absent a clear demarcation of where that authorization ends. In *Rodriguez*, for example, the employee exceeded his authorized access when he accessed his employer's database to obtain information for personal reasons because the employer's policy prohibited access for non-business reasons. 628 F.3d at 1261, 1263. That situation was different, this Court explained, from one where an employee with authorized access obtained information for personal reasons but the employer did not have a policy prohibiting access for those reasons. *Id.* (addressing *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)).

Again, it strains reason to suggest that an account owner could exceed her authorized access to the account. In any event, Sartori never communicated to Schrodt the extent to which she was authorized to use Skype. *See, e.g.*, App. 105. He never told her that she could not use the account or that she could do so only for specific purposes. Because Schrodt was authorized to access Skype and did not—indeed, could not—exceed her authorization, she did not violate the SCA or the CFAA by accessing Skype.

---

been limited because she was the account creator. As a result, she did not access any files or data that weren't encompassed by her initial authorization, and so Schrodt prevails under both this Court's approach in *Rodriguez* and the narrower approach.

B. Schrodt was authorized to access the Gmail account.

Schrodt accessed the Gmail account twice, on April 5 and May 6, 2016, each time without having to enter a password. *See* App. 151; *see also id.* at 85-86 (¶¶ 12, 17). As we now show, Schrodt was authorized to access Gmail on both dates because she accessed the account on a shared computer without having to enter a password. She was also authorized to access the account on May 6 for the independent reason that Sartori knew about her April 5 access to Gmail and took no steps to block further access.

1. Schrodt was authorized to access Gmail on April 5 and May 6. To be protected by the SCA and the CFAA, a website "must be configured in some way so as to limit ready access by the general public." *See Snow v. DirecTV, Inc.,* 450 F.3d 1314, 1322 (11th Cir. 2006). That's sensible because a readily accessible website does not require any authorization, so a plaintiff cannot prove one of the elements—lack of authorization—essential to recovery under both statutes. In other words, if access to an online account is unprotected, then access cannot be unauthorized. This Court has observed that if the rule were otherwise, and by simply accessing an unprotected webpage "one is liable under the SCA, then the floodgates of litigation would open and the merely curious" would be subject to civil and criminal liability. *Id.* at 1321. So Schrodt cannot be liable for doing nothing more than typing in a web address (via a shared computer no less).

When Schrodt opened the Gmail website, she was not required to enter a password and instead was immediately taken to Sartori's inbox. App. 151; *see id.* at 85-86 (¶¶ 12, 17). No court has suggested that a person viewing her spouse's emails, via a shared computer, violates the CFAA or the SCA. Even outside the marital context, courts have found unauthorized access only when someone gained access by guessing a password,

see, e.g., *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991), or by otherwise circumventing software barriers, *see, e.g.*, *Power Ventures,* 844 F.3d at 1068. Schrodt did neither. She "typed in Gmail.com," and Sartori's emails "popped up because that particular account had never been logged out of." App. 151. Because the account was readily accessible in both April and May and Schrodt did not circumvent any password protection, she did not access the account without authorization.

2. Schrodt's May 6 Gmail access was lawful for another reason: Schrodt had implied consent to access Gmail, as the district court held. *See* App. 186.

a. To begin with, this Court may affirm on the implied-consent issue without reaching its merits because Sartori hasn't squarely placed the issue before this Court. It is therefore forfeited. *See Allied Med. Transp., Inc.*, 805 F.3d at 1009. Sartori may point to one lonely sentence in his opening brief to argue that he raised this issue: "Failure to change an account password once exposed does not mitigate liability under SCA." Sartori Br. 20 (citing *Hately v. Watts*, 917 F.3d 770, 774 (4th Cir. 2019)). But that fleeting statement is too obscure and unilluminating to avoid a forfeiture. *See APA Excelsior III L.P. v. Premiere Techs., Inc.*, 476 F.3d 1261, 1270 (11th Cir. 2007).

b. Turning to the merits, implied authorization is fatal to a claim under the CFAA and the SCA. *See Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 757 (N.D. Ohio 2013) (citing *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir. 1993)). Sartori testified that he "wasn't worried at all" about Schrodt having "any additional access or anything like that" after the initial April 5 access because, at that point, the "cat was already out of the bag"—referring to the profane emails and his extramarital affairs. *See* D. Ct. Order, App. 186. As the district court put it, when Schrodt confronted Sartori about her discovery, he

"had every reason to believe that she would access the accounts again and no reason to believe that she wouldn't." *Id.* at 186 n.7. "And yet he testified … that he didn't change the passwords (nor did he even log out of the Gmail account!)." *Id.* Sartori never even told Schrodt not to access the account again. *See id.* at 106-07. That constitutes implied consent. *Cf. United States v. Workman*, 80 F.3d 688, 693-94 (2d Cir. 1996) (finding implied consent under federal wiretap statute where prison handbook put prisoner on notice that prisoners' calls are monitored); *Griggs-Ryan v. Smith*, 904 F.2d 112, 118-19 (1st Cir. 1990) (same with respect to federal and state wiretap statutes).

If Sartori's cryptic citation to *Hately*, 917 F.3d at 774, *see* Sartori Br. 20, is an attempt to excuse his inaction, that attempt would be misguided. Unlike here, the person charged in *Hately* with violating the CFAA was never authorized to access the email account. *See* 917 F.3d at 774. Rather, the plaintiff had shared his email password with his then-girlfriend, who in turn shared the password, *without authorization*, with another man, enabling him (the defendant) to access the plaintiff's email account. *See id.* By contrast, Schrodt had initial authorization, and she didn't access a stranger's email account using a password she wasn't supposed to have. *See* App. 85-86 (¶¶ 12, 17), 151.

3. The marital context here reinforces the conclusion that Schrodt's conduct—viewing password-unprotected emails, on a shared computer, in the marital home—was not unauthorized activity under the CFAA or the SCA. To be sure, spousal liability is not barred under these laws. *See Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 959, 961 (11th Cir. 2016). But spousal relationships are different from many others, and they often are characterized by everyday authorizations of the type at issue here. Spouses frequently share mutual understandings that they can use and access joint property—

cars, closets, computers—without requiring each other's perpetual affirmative consent. To overlook the distinct nature of authorization in the marital context is to flout reality.

The CFAA and the SCA were designed to criminalize cyber hacking, not spouses reading each other's emails. "A Gmail account that is unprotected by a password and accessible on the family's home computer would appear to be accessible to the other spouse just as the files on the hard drive." David H. Tennant & Michael G. McCartney, *Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical, and Technical Traps*, 24 No. 1 Prof. L. 13, 25 (2016). And so, when "access is full to both spouses and not password protected, there is no violation of the act, because the access was not 'without authorization.'" Laura W. Morgan, *Marital Cybertorts: The Limits of Privacy in the Family Computer*, 20 J. Am. Acad. Matrim. L. 231, 239 (2007).

Courts have understood that the marital context is more likely than others to give rise to authorization. In *White v. White*, 781 A.2d 85, 90-91 (N.J. Super. Ct. 2001), for example, the court held that the defendant was authorized to access emails stored on a couple's home computer, even though she did not use the computer frequently, because she did not have to enter a password and instead retrieved the emails off the computer's hard drive by searching through different file directories. Likewise, in *Byrne v. Byrne*, 650 N.Y.S.2d 499, 499-500 (N.Y. Sup. Ct. 1996), the court likened a shared home computer to a file cabinet in the marital residence, which both spouses are equally authorized to access, and concluded that the defendant had authority to access even password-protected files.

* * *

In sum, Schrodt was authorized to access the Gmail account because she did not have to enter a password or jump through other technological hoops to view the emails. And because Schrodt was also authorized to access Skype, all of Sartori's claims under the CFAA and the SCA fail. It is therefore not necessary for this Court to address whether Sartori met the $5,000-loss requirement under the CFAA or whether opened emails are held in electronic storage under the SCA. But, as demonstrated below, Sartori's claims fail on these grounds as well.

II. Schrodt did not violate the CFAA because Sartori did not incur any losses, let alone the $5,000 in losses required to trigger CFAA liability.

Sartori has not met the CFAA's loss requirement as a matter of fact and law. First, he has not pointed to any record evidence showing that he suffered any losses by reason of Schrodt's allegedly unauthorized access. Second, the types of losses Sartori claims to have suffered—the litigation costs of this case and costs from a separate divorce proceeding—are not cognizable losses under the CFAA.

A. Sartori failed to produce summary-judgment evidence that he suffered any losses.

Under the CFAA, Sartori was required to show that Schrodt's conduct caused him losses of at least $5,000. *See* 18 U.S.C. § 1030(g), (c)(4)(A)(i)(I). At summary judgment, Sartori asserted that Schrodt's allegedly unauthorized access to the Skype and Gmail accounts caused him losses in the form of litigation costs during his divorce proceedings and costs incurred to "remediat[e]" his computer system. *See* App. 139. The district court held that Sartori did not meet the loss requirement because he did not point to

any record evidence showing any losses. *Id.* at 190. Instead, the district court observed, Sartori's claim of losses was "all attorney argument." *Id.*

Sartori has now abandoned the argument that he incurred costs by having to remediate his computer systems, which was contradicted by Sartori's own deposition. *See* D. Ct. Order, App. 190-91. He asserted below that he hired a computer expert for $3,000 (still not enough to meet the $5,000 loss threshold), but he did so not to analyze the "cyber strike" and assess damages, as his counsel had argued. *See id.* Rather, he hired the expert only to gather evidence to litigate this case. *Id.* at 191 & n.9. The district court therefore concluded that "there is no actual evidence of any loss here at all, let alone $5,000 worth." *Id.* at 191.

Sartori still insists that he met the loss requirement because of the costs he incurred during his divorce proceedings. *See* Sartori Br. 23. As explained below (at 23-26), these costs do not constitute cognizable damages under the CFAA. In any event, as the district court held, Sartori does not point to any record evidence to support his alleged losses. App. 190.

Having abandoned his claim for remediation costs, and unable to provide evidence with respect to the divorce proceedings, Sartori now provides a new theory, namely that his litigation costs in *this* case count as CFAA losses. Sartori Br. 23. This Court should decline to address a claim raised for the first time on appeal. *See Access Now, Inc. v. Sw. Airlines Co.*, 385 F.3d 1324, 1330-35 (11th Cir. 2004). In any case, because this argument is new, Sartori did not (of course) provide any summary-judgment evidence below establishing his litigation costs in this case. Sartori thus failed to prove the $5,000 in losses necessary to sustain his CFAA claim.

B. The costs of a divorce proceeding or litigating an alleged CFAA violation are not losses under the Act.

Even if Sartori had offered evidence that he incurred $5,000 litigating this case and the divorce proceeding (which, again, he did not), these costs would not have constituted cognizable losses under the CFAA.

1. Sartori's argument that litigation costs are cognizable losses under the CFAA runs headlong into the relevant statutory language, which defines "loss" as:

> Any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11).

This statutory definition includes two separate types of losses: first, the reasonable costs incurred in connection with activities such as responding to an offense, conducting a damage assessment, and restoring the affected data; and, second, the reasonable costs associated with consequential damages resulting from interruption of service. *See Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1174 (11th Cir. 2017). The plaintiff need not prove interruption of service to recover for the direct costs of responding to the violation. *Id.* But to be entitled to consequential damages, the plaintiff must prove that the defendant's actions interrupted his computer services. *See id.*

Sartori's claim for CFAA damages suffers from multiple legal flaws. For starters, his alleged losses would be consequential damages under the CFAA, if they were cognizable losses at all. Consequential damages, such as lost revenue, are "[l]osses that do not flow

directly and immediately from an injurious act"—here, the purportedly unauthorized computer access—"but that result indirectly from the act." *Damages*, Black's Law Dictionary (11th ed. 2019). But Sartori cannot recover consequential damages under the CFAA because Schrodt's actions did not cause any service interruption. *See, e.g.*, *Nexans Wires S.A. v. Sark-USA, Int'l*, 166 F. App'x 559, 562-63 (2d Cir. 2006) (holding lost profits caused by misappropriation of confidential data were not recoverable under the CFAA because it was "undisputed that no interruption of service occurred"). That should end the inquiry—that is, because Sartori seeks consequential damages but cannot show any interruption of service as required by the CFFA, Sartori's CFAA claim fails.

If Sartori chooses to press on, he would be left to argue that his losses are covered by the first category of the CFAA's "loss" definition. This first category, however, even more plainly does not cover the types of losses Sartori alleges here. The phrase "any reasonable cost to any victim" is narrowed by the subsequent phrase, which lists a distinct category of losses directly associated with unauthorized computer access: responding to a CFAA offense, conducting a damage assessment, and restoring the system or its data to their condition prior to the offense. *See* 18 U.S.C. § 1030(e)(11); *see also Brown Jordan Int'l*, 846 F.3d at 1174. That is, the examples listed in Section 1030(e)(11) all concern costs related to investigating and remedying damage to the computer or relevant data—remediation that is sometimes required in the immediate aftermath of unauthorized computer access.

Sartori's position—that "any reasonable cost" can cover costs stemming from a separate divorce proceeding or costs incurred from litigating the alleged CFAA

violation itself—overlooks Congress's express limitation of the general term "any reasonable cost" to "the direct costs of responding to the violation in the first portion of the definition." *Brown Jordan Int'l*, 846 F.3d at 1174. "Any reasonable cost" therefore does not encompass costs as unrelated to remediation costs as Sartori's litigation expenses.

2. Courts have unanimously understood Section 1030(e)(11) this way and declined to recognize litigation costs as recoverable under the CFAA. *See, e.g.*, *Wichansky v. Zowine*, 150 F. Supp. 3d 1055, 1071-72 (D. Ariz. 2015). Thus, fees paid to a computer expert solely to assist in litigating a CFAA violation cannot count towards the loss requirement. *See, e.g.*, *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 338-39 (E.D. Pa. 2013); *Mintz v. Mark Bartelstein & Assocs., Inc.*, 906 F. Supp. 2d 1017, 1029-31 (C.D. Cal. 2012).

For example, in *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands, Inc.*, 616 F. Supp. 2d 805, 811-12 (N.D. Ill. 2009), the plaintiff was not concerned with the integrity of its data, provided no evidence of computer-system damage, and hired a computer expert only to assist in his CFAA lawsuit, not to conduct a damage assessment arising from unauthorized access to its database. *Id.* The costs the company incurred to pay the computer expert therefore did not constitute a loss under the CFAA. *Id.* So too here. Sartori acknowledged that he hired the computer expert solely for purposes of this lawsuit (not to fix the marital computer or to recover the data on it). App. 107.

Two decisions with contrasting results also help illustrate our point. In *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), Facebook suffered a loss under Section 1030(e)(11) because it was "undisputed that Facebook employees spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to"

the defendant's unlawful access. *Id.* at 1066. On the other hand, in *Nexans Wires*, 166 F. App'x at 562-63, the plaintiff failed to demonstrate that its travel expenses, incurred by sending its employees to investigate the misappropriation of certain stored data, were connected to "any type of computer investigation" or "preventative security measures," and thus did not constitute a CFAA loss. Certainly, then, if costs incurred from investigating business losses from data misappropriation cannot constitute CFAA losses, then costs incurred in an entirely separate divorce proceeding, or in litigating the alleged CFAA violation itself, do not fall within the statutory loss definition.

3. This conclusion—that CFAA "losses" do not include litigation costs—is underscored by the understanding that, in enacting the CFAA, Congress was operating against the backdrop of the time-honored "American Rule": that the costs of litigation, including attorney's fees, generally may be awarded only if a statute explicitly authorizes them. *See Alyeska Pipeline Serv. Co. v. Wilderness Soc'y*, 421 U.S. 240, 269 (1975); *Peter v. Nantkwest, Inc.*, 140 S. Ct. 365, 371 (2019) ("This Court has never suggested that any statute is exempt from the presumption against fee shifting."). In other words, litigation costs are not subsumed within a general damages award—like the general damages award authorized by the CFAA—when the statute does not expressly provide for them. *See Peter*, 140 S. Ct. at 373. Sartori's claim to litigation costs under the CFAA, then, ascribes to Congress an intent directly at odds with the American Rule. For that reason as well, Sartori's CFAA claim should be rejected.

III. Schrodt did not violate the SCA because the copies of Sartori's opened messages that she read were not held in "electronic storage."

Sartori's SCA claims are meritless not only because Schrodt was authorized to access the Gmail and Skype accounts, but also because the copies of the messages that Schrodt viewed were not held in "electronic storage." We refer here to message *copies* to underscore that any communication a user reads through an electronic messaging service is invariably one of many copies of the original communication created by the service provider, like Skype or Gmail. *See, e.g.*, *Hately v. Watts*, 917 F.3d 770, 791-93 (4th Cir. 2019). As shown below, whether the SCA applies to any message copy depends on the circumstances under which *that copy* is retained on a provider's servers.

The SCA prohibits anyone from intentionally accessing, without authorization, electronic messages while they are in "electronic storage." *See* 18 U.S.C. § 2701(a). As relevant here, the Act defines "electronic storage" as any storage (1) "by an electronic communication service" (2) "of such communication" (3) "for purposes of backup protection." *See id.* § 2510(17)(B).

The district court held that Schrodt could not be liable under the SCA because the message copies she read were not in "electronic storage" given that they had already been received and opened by Sartori. App. 198. The court found it "undisputed that all the emails had been opened" by the time Schrodt viewed them, *id.* at 182 & n.3, based on Schrodt's uncontradicted affidavit that "all of the emails and Skype transcripts that I read had previously been read by Plaintiff [Sartori]." *Id.* at 85 (¶ 13).

Sartori disagrees, arguing that copies of opened messages are in "electronic storage." Sartori Br. 10-20. As we now explain, the district court was right: Stored copies of

opened messages, like those Schrodt read, fall outside all three elements described above. Only communications awaiting transmission—whether in a copy to be delivered or a copy created to protect against data loss in transmission—are in "electronic storage." Any communication stored after it has been delivered and opened is not.[3]

A. An "electronic communication service" does not provide storage for copies of already-opened electronic messages.

1. Copies of opened messages retained on remote provider servers, like the messages read by Schrodt, are not held "by an electronic communication service" and, therefore, are not in "electronic storage" under 18 U.S.C. § 2510(17)(B). For that reason alone, Schrodt could not have violated the SCA.

Whether a service provider is delivering a service defined in the SCA is determined by looking to the context in which each copy of a message is held. *See Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 964 n.5 (11th Cir. 2016); *Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1215-16 (2004). That is,

---

[3] This result is consistent with the "majority view," which holds that "once the user of an entirely web-based email service … opens an email he has received, that email is no longer 'in electronic storage' on an electronic communication service." *In re Warrant to Search Certain Email Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 228 n.4 (2d Cir. 2016) (Lynch, J., concurring) (collecting cases), *vacated as moot by United States v. Microsoft Corp.*, 138 S. Ct. 1186, 1188 (2018); *see, e.g.*, *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); *see also Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1217 & n.61 (2004). *But see Hately v. Watts*, 917 F.3d 770, 797 (4th Cir. 2019); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004); *see also Clare v. Clare*, No. 19-36039, 2020 WL 7222150, at *3-4 (9th Cir. Dec. 8, 2020).

"the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract." Kerr, 72 Geo. Wash. L. Rev. at 1215. As a result, a provider may be employing one type of service for a given message copy at one time and another type of service at another time. *Vista Mktg.*, 812 F.3d at 964 n.5.

When Schrodt read the messages that Sartori had already opened, Skype and Gmail were not holding the copies she read as part of an "electronic communication service," which offers users only the "ability to send or receive … electronic communications." 18 U.S.C. § 2510(15). Transmitting emails and other electronic messages is, indisputably, an example of an "electronic communication service." *See, e.g.*, *Vista Mktg.*, 812 F.3d at 963-64. But after the communication has been delivered and opened, the provider's retention of any copy of that data no longer facilitates "send[ing] or receiv[ing]" the communication and therefore is no longer employing an "electronic communication service." *See United States v. Weaver*, 636 F. Supp. 2d 769, 772-73 (C.D. Ill. 2009).

Instead, once a copy of a message is received and opened, retention of any copy by the messaging provider is part of a different type of service—a "remote computing service"—which is defined under the SCA as "storage or processing services." *See* 18 U.S.C. § 2711(2); *Weaver*, 636 F. Supp. 2d at 772-73. Cloud-based storage is an example of a "remote computing service." *See Hately*, 917 F.3d at 790. Once an electronic message has been delivered and opened, any continued indefinite retention of message copies becomes exactly that—cloud-based "storage"—and so it leaves the realm of "electronic communication service" and enters "remote computing services." *See Weaver*, 636 F. Supp. 2d at 771-73; *Flagg*, 252 F.R.D. at 362-63; *see also Anzaldua v. Ne.*

Ambulance & Fire Prot. Dist., 793 F.3d 822, 842 & n.8 (8th Cir. 2015) (holding that sent emails were retained as part of a "remote computing service"); Kerr, 72 Geo. Wash. L. Rev. at 1213-14 (explaining in detail the difference under the SCA between an "electronic communication service" and a "remote computing service").

Message copies stored by a "remote computing service" are not in "electronic storage" because, in defining that term, Section 2510(17)(B) requires information in "electronic storage" to be held "by an electronic communication service." The SCA's text ends the inquiry: The message copies at issue here were held by a "remote computing service," not an "electronic communication service" and, thus, were not in "electronic storage," foreclosing Sartori's SCA claims.

2. The SCA's basic architecture, through which its privacy protections operate, also demands this result. As we explain further below, the SCA's distinction between electronic communication and remote computing services is a core feature of the Act's structure and is "essential" to its protections against service-provider disclosure of, and government access to, sensitive private data. *See In re Application of the United States of Am. for a Search Warrant, etc.*, 665 F. Supp. 2d 1210, 1214 & n.1 (D. Or. 2009).

For this reason, post-transmission storage cannot operate as both an "electronic communication service" and a "remote computing service" at the same time for a single message copy. *See Am. Health, Inc. v. Chevere*, No. CV-12-1678, 2017 WL 6561156, at *8 n.4 (D.P.R. Dec. 22, 2017) (citing Kerr, 72 Geo. Wash. L. Rev. at 1217 n.61). *Contra Hately*, 917 F.3d at 788-89. If it could, the SCA's critical distinction between the two services would collapse and undermine the Act's privacy protections. *See Anzaldua*, 793 F.3d at 842 n.8; *In re Application*, 665 F. Supp. 2d at 1214 & n.1.

This conclusion flows from SCA requirements that determine when service providers must protect the privacy of user information and when the government can compel disclosure of that information. *See* 18 U.S.C. §§ 2702(a), 2703(a)-(b). Copies of communications in "electronic storage" for 180 days or less as part of an "electronic communication service" may be disclosed only after a court issues a warrant supported by probable cause, but copies of communications stored on behalf of subscribers or customers as part of a "remote computing service" can be disclosed via subpoena based on a significantly less-stringent proof requirement. *See id.*; *see also In re Warrant*, 829 F.3d 197, 207-08 (2d Cir. 2016), *vacated as moot by United States v. Microsoft Corp.*, 138 S. Ct. 1186, 1188 (2018); *United States v. Warshak*, 631 F.3d 266, 283 (6th Cir. 2010); Kerr, 72 Geo. Wash. L. Rev. at 1218-19, 1223.

"Electronic communication services" and "remote computing services" must be mutually exclusive or the privacy-protecting benefits of a court warrant for "electronic communication services" would be eviscerated. If a provider could offer both services at the same time for a single message copy, the government could routinely obtain private communications through a mere subpoena, as permitted for "remote computing services," that should only be obtained through a court-approved warrant supported by probable cause. *See Am. Health*, 2017 WL 6561156, at *8 n.4 (citing Kerr, 72 Geo. Wash. L. Rev. at 1217 n.61).

In sum, the permanent retention of already-opened message copies on a provider's servers is not an "electronic communication service." On this basis alone, Sartori's messages were not held in "electronic storage" under 18 U.S.C. § 2701, and, therefore, Schrodt cannot be held liable under the SCA.

B. Copies of opened messages are not copies of "such communications."

1. Sartori's SCA claims also fall short because copies of his opened messages were not copies of "such communications" as used in Section 2510(17)(B). "Such communications" could be interpreted to refer to two phrases: all of the text in Section 2510(17)(A) or just the short phrase "wire or electronic communication" within Section 2510(17)(A). The ordinary meaning of "such" and its use in the definition of "electronic storage" demonstrate that "such" refers to the whole of Section 2510(17)(A). For that reason, "such communication" means only those message copies in "temporary, intermediate storage … incidental to the electronic transmission thereof." *See* 18 U.S.C. § 2510(17)(A).

And because "temporary, intermediate storage … incidental to the electronic transmission thereof" extends only to message copies in transmission (and not to opened message copies), copies of already-opened messages are not copies of "such communications" and, therefore, are excluded from Section 2510(17)(B). *Cf. Jennings v. Jennings*, 736 S.E.2d 242, 247-48 (S.C. 2012) (Toal, C.J., concurring) (concluding that "electronic storage refers only to temporary storage, made in the course of transmission, by an ECS provider, and to backups of such intermediate communications" because Section 2510(17)(A) limits the reach of Section 2510(17)(B)).

Again, the SCA defines "electronic storage" as:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of *such communication* by an electronic communication service for purposes of backup protection of *such communication*.

18 U.S.C. § 2510(17) (emphasis added). It is undisputed that copies of opened messages, and therefore the message copies at issue here, are not in "temporary, intermediate storage … incidental to the electronic transmission" under Section 2510(17)(A). *See, e.g.*, *Hately*, 917 F.3d at 785; *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003). Simply put, once one copy of a message is opened, no copy of the message can be held incident to transmission because transmission is complete. *Id.*

"Such communication" in Section 2510(17)(B) refers back to the entire description of the "communication" set forth in Section 2510(17)(A), and it therefore does not include copies of opened messages. "Such" refers to the "character, degree, or extent" of the thing previously described, unless otherwise indicated. *See Such*, Oxford English Dictionary (3d ed. 2020). Nothing indicates otherwise here. There is no structural, typographical, or logical separation between the described storage attributes and the rest of the text in part (A). Put another way, if "such" in part (B) were less encompassing, it would fail to refer to the "character, degree, or extent" of the thing described in part (A). Therefore, the most sensible reading of (B) is that its use of "such" refers back to the entire "communication" described in (A).

Context reinforces the conclusion that "such" incorporates the full meaning of "communication" set forth in part (A). Both (A) and (B) form part of the definition of

"electronic storage" within Section 2510(17). Storage attributes are thus the most important characteristics described in (A) and (B). It would be illogical for "such" to exclude the *storage attributes* described in part (A), unless explicitly stated, because they are central to the meaning of "electronic *storage*."

Put differently, the "storage" attributes described in (A)—"temporary, intermediate … incidental to the electronic transmission"—are not separate, divisible concepts, but part of a unified phrase that makes sense only when read together. Those attributes modify "communication" just as much (and as importantly) as the phrase "wire or electronic" modifies "communication" elsewhere in part (A). If Congress had intended Section 2510(17)(B) to apply only to the clipped phrase "wire or electronic communication," as some courts have mistakenly held, *see, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066, 1076 (9th Cir. 2004), it would have said so by using in part (B) the simple language "any storage of a wire or electronic communication" rather than employing "such" to refer back to only three words in part (A). Congress would not have done that, because then "such" would be doing almost no work.

In sum, retaining a copy of an opened message does not amount to backup protection storage of "such communication" under Section 2510(17)(B) because "temporary, intermediate storage … incidental to the transmission" under Section 2510(17)(A) does not extend to storage of opened message copies.

2. Some courts have concluded that if "such" in part (B) referred to the entire text in part (A), that would render part (B) superfluous. That is, if our understanding of "such" were correct, then part (B) would cover the same stored message copies as part (A) because any message copy stored for "backup protection" under part (B) would be

in "temporary, intermediate" storage and therefore satisfy part (A). *See Hately*, 917 F.3d at 787; *Theofel*, 359 F.3d at 1075-76.

That reasoning is simply wrong. A backup copy held under part (B) is distinct from a message copy held under part (A) because part (B) storage is not "incidental" to transmission. *See Anzaldua*, 793 F.3d at 840 n.7 (quoting Kerr, 72 Geo. Wash. L. Rev. at 1217 n.61). Storage under part (B) serves a different purpose: "backup protection." In other words, message copies stored under part (B) have no transmission purpose because service providers do not intend to deliver them. Absent part (B), regularly created copies of unopened messages would be "unprotected by the SCA." *Id.* Thus, under our understanding of "such," Part (B) serves its own, critical purpose.

In sum, backup copies of already-transmitted messages, like Sartori's, are not "such communications" and therefore are not in "electronic storage" under part (B). Sartori's SCA claims should be rejected for that reason as well.

C. "Backup protection" storage is limited to copies of messages awaiting transmission, not copies of already-opened messages.

Sartori's SCA claims misfire for another reason: Copies of his already-opened messages were not held for "backup protection," as the district court correctly held. App. 194-98.

1. The text surrounding "backup protection" in Section 2510(17)(B) narrows that term's scope to storage of backup copies to facilitate transmission and does not extend to storage post-transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, rev'd in part on other grounds*, 352 F.3d 107 (3d Cir. 2003). Something stored for "backup protection" must be a duplicate copy held to ensure

continued access to a message should other copies be damaged or otherwise made inaccessible. *See To back up*, Oxford English Dictionary; *Protect*, Oxford English Dictionary. The terms adjacent to "backup protection" demonstrate that, under the SCA, the relevant "other copies" must be awaiting transmission and not be retained permanently after being opened. Not only must the backup copy be of "such communications," but it must also be held "by an electronic communication service." 18 U.S.C. § 2510(17)(B). For the reasons stated above in III.A & B, both phrases require that copies stored under part (B) support message transmission and therefore exclude copies of opened messages.

2. Congress must have temporally limited "backup protection" in this manner to avoid overbroad constructions of the Wiretap Act. When the SCA was enacted in 1986, Congress also amended the Wiretap Act to expand the types of communications that it was unlawful to "intercept." *United States v. Steiger*, 318 F.3d 1039, 1047-48 (11th Cir. 2003). These communications included "electronic communications" in transit and "wire communications" in "electronic storage," as then defined in Section 2510(17). *Id.* Before the 1986 amendment, an "intercept" required "acquisition of a communication contemporaneous with transmission." *Id.* at 1047. It is implausible that the Wiretap Act would have applied to wire communications held permanently because the contemporaneousness requirement of "intercept" would have been meaningless. *See Fraser*, 135 F. Supp. 2d at 635 (holding that interception of wire communications held in electronic storage occurs only until the communication is received and opened).

3. The notion that opened messages could exist in "backup protection" creates another textual anomaly. Extending "backup protection" to message copies held

indefinitely after a message has been opened would give "backup protection" the same meaning as "storage," effectively changing the text of Section 2510(17)(B) to "storage … for purposes of [storage]." *Cf. Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013) (holding that "backup protection" is narrower than storage).

To explain: To "store" something means to "retain a physical representation of" data "that enables them to be subsequently retrieved." *Store*, Oxford English Dictionary. This definition would wholly subsume "backup protection" if that phrase were given a broad meaning that includes stored copies of opened messages. First, the purpose of a message's retention would always be the same. In each case, a message would be retained to ensure future access and would necessarily protect against a lack of future access to other copies for any reason. Second, the requirement that "backup protection" rely on duplication does not distinguish it from "storage" given how the internet operates in practice. It is invariably the case that when electronic data is retained, duplicates are created. All service providers routinely create copies of communications as their primary protection against data loss. *See Anzaldua*, 793 F.3d at 840 n.7. As a result, no message would ever be held consistent with the definition of "storage" alone because every retained message will be a duplicate that qualifies it as "backup protection."

4. The SCA's narrow focus on the security of electronic messages held on service providers' servers during the transmission process—but not after the messages have been opened by the recipient—does not leave individuals without recourse against cyber hackers and government intrusion, nor does it herald the end of internet privacy. The CFAA criminalizes unauthorized access to nearly any computer, including third-party servers, to obtain stored files like opened emails. *See* 18 U.S.C. § 1030. And the

Department of Justice no longer seeks email contents without a warrant in light of a Sixth Circuit decision holding that Fourth Amendment protections apply to email contents. *See In re Warrant*, 829 F.3d at 222 n.1 (Lynch, J., concurring); *Warshak*, 631 F.3d at 288.

* * *

In sum, "backup protection" under the SCA is limited to ensuring continued access to messages awaiting transmission and does not cover opened messages. So Sartori's opened messages were not in "electronic storage," and for that reason as well, Sartori's SCA claims against his ex-wife are meritless.

CONCLUSION

The district court's judgment should be affirmed.

Respectfully submitted,

Hannah M. Beiderwieden
Student Counsel
Colin P. Shannon
Student Counsel

/s/Brian Wolfman
Brian Wolfman
GEORGETOWN LAW APPELLATE
COURTS IMMERSION CLINIC
600 New Jersey Ave., NW, Suite 312
Washington, D.C. 20001
(202) 661-6582
wolfmanb@georgetown.edu

Larry A. Matthews
Raymond F. Higgins, III
MATTHEWS & HIGGINS, LLC
114 East Gregory Street
Post Office Box 13145
Pensacola, FL 32591-3145
(850) 434-2200

Counsel for Plaintiff-Appellant Julie Schrodt

December 14, 2020

CERTIFICATE OF COMPLIANCE

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 10,884 words.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and type-style requirements of Fed. R. App. P. 32(a)(6) because this document has been prepared in a proportional-spaced typeface using Microsoft Word 2016 in Garamond font in 14 point type.

/s/Brian Wolfman
Brian Wolfman

December 14, 2020

STATUTORY ADDENDUM

Table of Contents

18 U.S.C. § 1030. Fraud and related activity in connection with computers

(a) Whoever—

* * *

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

* * *

(C) information from any protected computer;

* * *

shall be punished as provided in subsection (c) of this section.

* * *

(c) The punishment for an offense under subsection (a) or (b) of this section is—

* * *

(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

* * *

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

* * *

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

* * *

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or

* * *

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

* * *

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

* * *

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;

* * *

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and

injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

* * *

18 U.S.C. § 2701. Unlawful access to stored communications

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

* * *

18 U.S.C. § 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

* * *

18 U.S.C. § 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

* * *

18 U.S.C. § 2510. Definitions

As used in this chapter—

* * *

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(17) "electronic storage" means--

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

* * *

CERTIFICATE OF SERVICE

I certify that, on December 14, 2020, this brief was filed using the Court's CM/ECF system. All participants in the case are registered CM/ECF users and will be served electronically via that system.

/s/Brian Wolfman
Brian Wolfman