PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-1306

PATRICK HATELY, an individual,

Plaintiff – Appellant,

v.

DR. DAVID WATTS, an individual,

Defendant – Appellee.

THE CENTER FOR DEMOCRACY & TECHNOLOGY; THE ELECTRONIC FRONTIER FOUNDATION; NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE,

Amici Supporting Appellant,

DIGITAL JUSTICE FOUNDATION,

Amicus Supporting Appellee.

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. Anthony J. Trenga, District Judge. (1:17-cv-00502-AJT-JFA)

Argued: October 30, 2018 Decided: March 6, 2019

Before GREGORY, Chief Judge, MOTZ and WYNN, Circuit Judges.

Reversed and remanded by published opinion. Judge Wynn wrote the opinion, in which Chief Judge Gregory and Judge Motz joined.

ARGUED: Eric James Menhart, LEXERO LAW, Washington, D.C., for Appellant. Jonathan David Frieden, ODIN, FELDMAN & PITTLEMAN, P.C., Reston, Virginia, for Appellee. **ON BRIEF:** James P. Miller, ODIN, FELDMAN & PITTLEMAN, P.C., Reston, Virginia, for Appellee. Marta F. Belcher, James R. Batchelder, Monica A. Ortel, James H. Rickard, East Palo Alto, California, Evan Gourvitz, Lance W. Shapiro, New York, New York, Kathryn C. Thornton, ROPES & GRAY LLP, Washington, D.C.; Gregory T. Nojeim, CENTER FOR DEMOCRACY & TECHNOLOGY, Washington, D.C.; Andrew Crocker, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California; Kevin Bankston, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, Washington, D.C., for Amici The Center for Democracy & Technology, The Electronic Frontier Foundation, and New America's Open Technology Institute. Andrew Grimm, DIGITAL JUSTICE FOUNDATION, Omaha, Nebraska, for Amicus The Digital Justice Foundation.

WYNN, Circuit Judge:

Patrick Hately brought this action alleging that David Watts unlawfully accessed messages in Hately's web-based email account in violation of the Virginia Computer Crimes Act and the federal Stored Communications Act. But the district court found that Hately failed to demonstrate the requisite statutory injury under state law, and that Hately's previously opened and delivered emails stored by a web-based email service were not in statutorily protected "electronic storage" under federal law. We disagree with both determinations and therefore reverse and remand this case to the district court for further proceedings consistent with this opinion.

I.

A.

In August 2008, Hately enrolled at Blue Ridge Community College ("Blue Ridge College"), a constituent institution of the Virginia Community College System. At Blue Ridge College, Hately had a student email account that he continued to use after he graduated in 2013.

Blue Ridge College uses a web-based email client with branding specific for Blue Ridge College. Google hosts all emails.[1] Account holders can access the copies stored

[1] Generally, email clients can be categorized as either: (1) web-based and (2) non-web-based. *See United States v. Weaver*, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009). For web-based clients, an email host stores the user's "emails and other personal information in the cloud." *Melissa Medina*, The Stored Communications Act: An Old Statute for Modern Times, 63 Am. U. L. Rev. 267, 287 (2013). The local user's own "computer or mobile device merely serves as a conduit to access the [host's] server." *Id.* at 273; *see also Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012). For non-web-based clients, (Continued)

on their web-based email page as long as the student does not delete those copies. Blue Ridge College also stores at least one additional copy of all student emails, which can be used to recover any email that is accidentally deleted. Students may access these stored copies only by requesting them from Blue Ridge College's technical support personnel.

From August 2011 to February 2015, Hately had an intimate relationship with Nicole Torrenzano ("Nicole"), with whom Hately has two children. During their relationship, Hately and Nicole shared login and password information for their email accounts—including Hately's Blue Ridge College email account. But when, about March 2015, Nicole informed Hately that she also was involved in an intimate relationship with Watts, who was her co-worker and married to Audrey Hallinan Watts ("Audrey"), Hately and Nicole separated. Pertinent to this action, Hately did not change the password that he shared with Nicole for his Blue Ridge College email account.

Watts and Nicole continued their personal relationship, and during the fall of 2015, Watts and Audrey initiated divorce proceedings. In an effort to help Watts in his divorce proceedings, Nicole told Watts that Hately and Audrey were having an affair. Nicole said she knew of emails between Hately and Audrey that Watts could obtain by using the password that she had to Hately's Blue Ridge College email account.

Watts stated that he used the password Nicole gave him to browse through Hately's emails but contended that he "did not open or view any email that was

---

users access their email by "downloading it [directly] onto their personal computers." *Weaver*, 636 F. Supp. 2d at 772 n.2. After the users download their email, the email host may or may not delete the email from the email host's server. *See id.*

unopened, marked as unread, previously deleted, or in the [student email account]'s 'trash' folder." J.A. 506. Watts also said that he did not "change the status of, or modify, any email in any way." *Id.*

B.

In September 2016, Hately filed his first lawsuit against Watts and Nicole in the United States District Court for the Eastern District of Virginia ("*Hately I*"), alleging that they unlawfully accessed his email, in violation of: (1) the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ; (2) the federal Stored Communications Act, 18 U.S.C. § 2701, *et seq.*; and (3) the Virginia Computer Crimes Act, Va. Code Ann. § 18.2-152.1, *et seq.* Shortly after filing suit, Hately voluntarily dismissed his claims against Watts, without prejudice, and amended his complaint against Nicole. In his amended complaint, Hately alleged that he "incurred actual damages by the illicit access because [he] was forced to incur damages in time invested, software purchases to track and prevent future access, and more[.]" J.A. 39 ¶ 93. He further alleged that he had "incurred many hours of valuable time away from day-to-day responsibilities in attempting to determine the source of the computer breach." J.A. 37 ¶ 76.

In an order dated December 2, 2016, the district court in *Hately I* dismissed "without prejudice" Hately's Computer Fraud and Abuse Act and Virginia Computer Crimes Act claims against Nicole. The order provided no explanation as to why the court dismissed those claims. But in a subsequent opinion addressing a different issue, the court explained: "[a]lthough [Nicole] moved to dismiss the [Virginia Computer Crimes Act] Claims on multiple grounds, the Court dismissed the [Virginia Computer Crimes

Act] Claims because [Hately] failed to sufficiently allege how he sustained any injury to person or property by reason of a violation of the [Virginia Computer Crimes Act]." *Hately v. Torrenzano*, No. 1:116-CV-01143 (GBL/MSN), 2017 WL 2274326, at *3 (E.D. Va. May 23, 2017). The district court did not dismiss Hately's Stored Communications Act claim.

On February 13, 2017, Hately moved to amend his complaint for a second time. This time, Hately sought to rename Watts as a defendant and to reinstate his Computer Fraud and Abuse Act and Virginia Computer Crimes Act claims against Nicole. The district court denied the motion *solely* on grounds that Hately's "attempt to amend the complaint would cause undue prejudice to [Nicole]." *Hately v. Torrenzano*, No. 1:16-CV-01143 (GBL/MSN), 2017 WL 1428712, at *1 (E.D. Va. Apr. 20, 2017). According to the court, amending the complaint "would certainly require the Court to reopen discovery for Watts" and would "change the nature of this litigation" by "add[ing claims] to what would otherwise be a narrow case involving a single cause of action under the Stored Communications Act[.]" *Id.* Hately did not appeal the *Hately I* court's denial of his motion to amend.

C.

In April 2017, Hately refiled his action against Watts, again alleging that Watts unlawfully accessed his email, in violation of the Computer Fraud and Abuse Act, the Stored Communications Act, and the Virginia Computer Crimes Act.

Unlike his initial action against Watts, which was voluntarily dismissed without prejudice, Hately's refiled action supported his Virginia Computer Crimes Act claims by

reciting additional factual allegations bearing on damages. *Hately*, 2017 WL 2274326, at *3. For example, whereas Hately's initial complaint alleged that Hately "incurred many hours of valuable time away from day-to-day responsibilities in attempting to determine the source of the computer breach," J.A. 37 ¶ 76, Hately's complaint in the refiled action provided greater detail as to the time he lost as a result of the breach, alleging that he "was forced to identify" and make "several calls to" Blue Ridge College's technical support personnel "in order to ascertain the individual(s) that owns the domain for his school-related email account, as well as the individual(s) that manages the exchange servers for his school-related email account." J.A. 165 ¶¶ 94–96. And Hately's refiled complaint alleged that he "review[ed]" "hundreds or thousands of email messages" and "restore[d]" "deleted but unread email messages" that "were previously unknown to [Hately]." J.A. 166 ¶¶ 97–98. Also, the refiled complaint alleged that Hately was "forced to download and run programs that scanned his mobile telephone for viruses." J.A. 170 ¶ 115.

After conducting a hearing on July 6, 2017, the district court dismissed the Virginia Computer Crimes Act claims against Watts for two independent reasons.[2] First, the court held that the Virginia Computer Crimes Act claims were barred by collateral estoppel. The court explained in an oral ruling that "[a]ll of the damages that [Hately] alleges in this [instant] action . . . were the subject of [a prior motion to dismiss in *Hately I*], and that issue was fully briefed and argued in open court in the prior proceedings."

[2] The district court also dismissed Hately's claim under the Computer Fraud and Abuse Act, but Hately does not appeal that dismissal.

J.A. 377. Even though the *Hately I* court dismissed the Virginia Computer Crimes Act claims "without prejudice," the district court concluded that the previous dismissal had "finally determined" that Hately had not "sustained injury to person or property" under the Virginia Computer Crimes Act. J.A. 382. Accordingly, the district court held that Hately was "estopped from relitigating those injury claims." *Id.* Second, the district court concluded that, even if collateral estoppel did not apply, Hately failed to plausibly allege statutory injury, notwithstanding that Hately's new complaint included additional factual allegations bearing on injury. J.A. 383 (holding that Hately had "not alleged facts that make plausible his claim that he has sustained injury to person or property as those terms have been construed under the [Virginia Computer Crimes Act]").

Thereafter, in January 2018, Hately and Watts filed cross-motions for summary judgment on the remaining Stored Communications Act claim. In an order entered March 14, 2018, the district court denied Hately's motion, granted Watts' motion, and dismissed the case. In an accompanying opinion, the court held that "previously opened and delivered emails" stored "in a web-based email client" were not in protected "electronic storage" for purposes of the Stored Communications Act. *Hately v. Watts*, 309 F. Supp. 3d 407, 408, 410–14 (E.D. Va. 2018). According to the court, the statutory definition of "electronic storage" "covers emails only up to the point where the emails have been initially transmitted to their recipient and read or initially downloaded." *Id.* at 410.

The district court also held that Hately's emails were not protected under the statute because they were not stored by an "electronic communication service" and were

not stored "for purposes of backup protection." *Id.* at 412–413 (quoting 18 U.S.C. § 2510(17)(B)). According to the court, Blue Ridge College was acting, for purposes of the Stored Communications Act, as a "remote computing service"—not as an "electronic communication service"—because the emails Watts accessed were "service copies" maintained by Blue Ridge College "for the purposes of transmitting them to a single user's account upon that user's command." *Id.* at 413. Furthermore, the emails were not stored for purposes of backup protection because, the court maintained, they were stored for *Hately's* backup purposes rather than *Blue Ridge College's* "own backup or administrative purposes." *Id.* Because Hately's accessed emails were not protected "electronic storage," Watts was entitled to judgment as a matter of law on the Stored Communications Act claim. *Id.*

Hately timely appealed the dismissal of his Virginia Computer Crimes Act claims and the grant of summary judgment on the Stored Communications Act claim. We address each claim in turn.

II.

Regarding the district court's dismissal of his Virginia Computer Crimes Act claims, Hately contends that the district court's error was twofold. First, that the court improperly applied the doctrine of collateral estoppel, also referred to as "issue preclusion," to bar reconsideration of whether he adequately alleged that his "property or person [was] injured" within the meaning of the Virginia Computer Crimes Act. *See* Va. Code Ann. § 18.2-152.12(A). And second, that the court incorrectly determined that he failed to plausibly allege injury to person or property within the meaning of the Virginia

Computer Crimes Act. We agree, and therefore conclude that the district court erred in dismissing Hately's Virginia Computer Crimes Act claims.

A.

The district court applied the doctrine of issue preclusion to bar reconsideration of whether Hately's complaint adequately alleged his "property or person [was] injured" within the meaning of the Virginia Computer Crimes Act. Va. Code Ann. § 18.2-152.12(A). Issue preclusion bars "successive litigation of an issue of fact or law actually litigated and resolved in a valid court determination essential to the prior judgment, even if the issue recurs in the context of a different claim." *Taylor v. Sturgell*, 553 U.S. 880, 892 (2008) (citation and alterations omitted); *see also Angstadt v. Atlantic Mut. Ins. Co.*, 457 S.E.2d 86, 87 (Va. 1995) ("The doctrine of collateral estoppel precludes parties to a prior action and their privies from litigating in a subsequent action any factual issue that actually was litigated and essential to a valid, final judgment in the prior action."). We review the application of issue preclusion de novo. *United States v. Fiel*, 35 F.3d 997, 1005 (4th Cir. 1994).

To determine whether the district court properly applied issue preclusion, we must determine which jurisdiction's preclusion law governs. *See Semtek Int'l v. Lockheed Martin Corp.*, 531 U.S. 497, 506–09 (2001) (citing, among others, *Erie R. Co. v. Tompkins*, 304 U.S. 64, 78–80 (1938)). Neither the Supreme Court nor this Court has ever addressed what law governs the issue-preclusive effect of a federal court disposition of a state law claim rendered in a case in which the federal court exercised supplemental jurisdiction over the state law claim. However, in *Semtek International v. Lockheed*

Martin, the Supreme Court held that when a federal court exercises diversity jurisdiction over a state law claim, "federal common law governs the claim-preclusive effect of a dismissal" of the state law claim by the federal court. 531 U.S. at 508. The federal preclusion rule in such cases is to apply "the law that would be applied by state courts in the State in which the federal diversity court sits" as long as the state rule is not "incompatible with federal interests." *Id.* at 508–09 (citations omitted). Federal courts apply state preclusion law because "there is no need for a uniform federal rule" in a state-law cause of action, the Court explained. *Id.* Indeed, an alternative federal rule would "produce the sort of forum shopping and inequitable administration of the laws that *Erie* seeks to avoid, since filing in, or removing to, federal court would be encouraged by the divergent effects that litigants would anticipate from likely grounds of dismissal." *Id.* (internal quotations and citations omitted).

These justifications are equally persuasive in cases in which federal courts exercise supplemental, as opposed to diversity, jurisdiction over state law claims. Accordingly, we hold that when a federal court exercises supplemental jurisdiction over a state law claim, federal common law governs the preclusive effect of the federal court's disposition of that claim. *Cf. id.* The federal rule of decision in such cases is to apply state preclusion law, unless the state preclusion law is incompatible with federal interests. *Cf. id.*; *accord Access 4 All Inc. v. Trump Int'l Hotel & Tower Condo.*, No. 04-CV-7497KMK, 2007 WL 633951, at *3 (S.D.N.Y. Feb. 26, 2007).

Here, we discern no reason why Virginia preclusion law is incompatible with federal interests. Applying state preclusion law here would not undermine "federal

courts' interest in the integrity of their own processes." *See Semtek Int'l.*, 531 U.S. at 509 (providing, as an example, that a state's failure to estop "willful violation[s] of discovery orders . . . might justify a contrary federal rule"). On the contrary, applying Virginia preclusion law furthers the "federalism principle of *Erie*" by ensuring there are not "substantial variations in outcomes between state and federal litigation which would likely influence the choice of a forum." *Id.* at 504 (internal quotations and alterations omitted); *see also Q Int'l Courier Inc. v. Smoak*, 441 F.3d 214, 218, 218 n.1 (4th Cir. 2006) (finding Virginia's claim preclusion law was "not incompatible with any federal interest" when state law would bar the plaintiff from relitigating a "common core of operative facts").

We thus apply Virginia preclusion law to determine whether the doctrine of issue preclusion barred Hately from litigating the adequacy of his allegations as to damages in his new complaint. Under Virginia law, a party asserting defensive issue preclusion has "the burden of proving that the claim or question had been in issue and determined in [a] prior . . . action." *Scales v. Lewis*, 541 S.E.2d 899, 901 (Va. 2001). Specifically, the proponent of issue preclusion must demonstrate that: "(1) the parties to the two proceedings, or their privies, be the same; (2) the factual issue[3] sought to be litigated must have been actually litigated in the prior action and must have been essential to the prior judgment; and (3) the prior action must have resulted in a valid, final judgment

[3] We assume, without deciding, that Virginia would apply issue preclusion to this question of law. *See Bates v. Devers*, 202 S.E.2d 917, 921 n.6 (Va. 1974) (stating issue preclusion "is applied with less rigor to issues of law" (citing Restatement of Judgments § 70 (1942); Restatement (Supp.) of Judgements § 70 (1948))).

against the party sought to be precluded in the present action." *Weinberger v. Tucker*, 510 F.3d 486, 491 (4th Cir. 2007) (citing *TransDulles Ctr., Inc. v. Sharma*, 472 S.E.2d 274, 275 (Va. 1996)). Also, "in Virginia, [issue preclusion] requires a fourth element, mutuality." *Id.* (citing *TransDulles Ctr.*, 472 S.E.2d at 275).

1.

As under federal preclusion law, Virginia applies the doctrine of issue preclusion only when the decided issue is "essential to the prior judgment." *See TransDulles Ctr.*, 472 S.E.2d at 275. Thus, when, as here, issue preclusion is "considered in the context of two separate litigations[,] if a judgment in the prior case is supported by either of two findings, neither finding can be found essential to the judgment." *In re Microsoft Corp. Antitrust Litig.*, 355 F.3d 322, 328 (4th Cir. 2004); *see Scales*, 541 S.E.2d at 901; *cf. Reid v. Ayscue*, 436 S.E.2d 439, 441 (Va. 1993) (holding that issue preclusion was appropriate when there was only one "rational interpretation" of a prior jury verdict).

Although the *Hately I* dismissal order did not explain why Hately's Virginia Computer Crimes Act claims were dismissed, the court later elaborated that Hately had "failed to sufficiently allege how he sustained any injury to person or property by reason of a violation of the Virginia Computer Crimes Act." *Hately*, 2017 WL 2274326, at *3. In rendering its oral ruling on issue preclusion, the district court in the instant case appears to have read this sentence as a determination that the three "categories" of damages Hately alleged—(1) "expenses incurred in connection with evaluating the defendant's alleged wrongful conduct," (2) expenses incurred in "reporting the alleged hacking to law enforcement," and (3) the cost of time spent "reviewing records, restoring

e-mails, and researching and implementing security enhancements"—were not, as a matter of law, actionable under the Virginia Computer Crimes Act. *See* J.A. 375–77 (holding that in his current "complaint, [Hately] alleged damages that fall within the three categories of damages" he set forth in his first action).

But the *Hately I* court's explanation for its decision to dismiss the Virginia Computer Crimes Act claims is as—if not more—plausibly read as holding *not* that the three "categories" of damages alleged were not actionable under the Virginia Computer Crimes Act, but rather, in the court's own words, that Hately's complaint failed to include "sufficien[t]," nonconclusory factual allegations establishing such damages to satisfy the requirements of Federal Rule of Civil Procedure 12(b)(6). *Hately*, 2017 WL 2274326, at *3; *see also Aziz v. Alcolac, Inc.*, 658 F.3d 388, 391 (4th Cir. 2011) ("[S]tatements of bare legal conclusions are not entitled to the assumption of truth and are insufficient to state a claim[.]"). That this Court has held that the "categories" of damages Hately alleged in his previous complaint *are* actionable under the Virginia Computer Crimes Act, *see infra* Part II.B, supports this reading of the *Hately I* court's order, as we presume that the district court correctly applied this Court's precedent. Accordingly, at a minimum, it is unclear whether the *Hately I* court dismissed the prior action because, as the district court below believed, the "categories" of damages Hately alleged were not actionable under the Virginia Computer Crimes Act or because the factual allegations bearing on damages lacked sufficient specificity to satisfy Rule 12(b)(6).

When, as here, a prior court's explanation for its grounds for dismissing a prior action is amenable to multiple interpretations, courts decline to hold that the prior court disposition has preclusive effect in subsequent litigation. For example, in *Mitchell v. Humana Hospital-Shoals*, the Eleventh Circuit considered whether a federal district court in a Title VII retaliatory constructive discharge case properly dismissed the action on grounds that the dismissal of a previous state worker's compensation case precluded the plaintiff from relitigating whether she had good cause for resigning her position. 942 F.2d 1581, 1582–83 (11th Cir. 1991). The Eleventh Circuit held that the district court erred in holding that the doctrine of issue preclusion barred the plaintiff from relitigating whether she had just cause to resign. *Id.* at 1583–84. In reaching this conclusion, the court emphasized that there were at least two reasons the prior court may have dismissed the earlier worker's compensation action: (1) the plaintiff lacked just cause to resign *or* (2) the plaintiff "had been unavailable for work since her resignation and had not made efforts to secure substitute employment." *Id.* at 1583. Because the prior court "entered a general order denying benefits without giving reasons in support and making findings of fact," it was unclear from the record which of these two reasons served as the basis for the prior court's decision to dismiss the action. *Id.* at 1583–84. Accordingly, issue preclusion did not apply because the record provided no basis to "be certain if the [prior] court actually decided whether [the plaintiff] had just cause to resign." *Id.* at 1584.

As explained above, just as in *Mitchell*, the *Hately I* court's one-sentence description of the basis of its dismissal of the Virginia Computer Crimes Act claims leaves open at least two possibilities as to the reason for the dismissal: (1) the court

concluded that the "categories" of damages Hately alleged were not, as a matter of law, actionable under the Virginia Computer Crimes Act *or* (2) the court concluded Hately failed to plead those damages with sufficient specificity. Accordingly, contrary to the district court's issue preclusion ruling, we "cannot be certain if the court actually decided whether" the categories of damages Hately alleged were not actionable under the Virginia Computer Crimes Act, barring application of the doctrine of issue preclusion. *Id.* Notably, Virginia courts likewise decline to apply issue preclusive effect to prior court dispositions subject to multiple interpretations. *See Pijor v. Commonwealth*, 808 S.E.2d 408, 411–12 (Va. 2017) ("Collateral estoppel does not apply if it appears that the prior judgment could have been grounded upon an issue other than that which the defendant seeks to foreclose from consideration." (internal quotation marks and alterations omitted)).

Significantly, Hately's complaint in the instant case includes numerous new and specific factual allegations pertaining to damages that Hately *did not allege* in the complaint that the *Hately I* court found insufficient, *see infra* Part II.B; *supra* Part I.C, meaning that the *Hately I* court did not have an opportunity to pass judgment on the sufficiency of the factual allegations at issue in this case. Accordingly, to the extent the *Hately I* court dismissed the Virginia Computer Crimes Act claims on grounds that the factual allegations in the complaint lacked the requisite specificity to satisfy Rule 12(b)(6), that determination would not preclude a holding that Hately's factual allegations pertaining to Virginia Computer Crimes Act damages in this case satisfied Rule 12(b)(6). *Cf. Loudoun Hosp. Center v. Stroube*, 650 S.E.2d 879, 887 (Va. App.

2007) (declining to apply doctrine of issue preclusion in permitting case because "[t]he distinctions . . . between the [first permit] application and the [second] application are such that the factual issues [of the first case] were not 'actually litigated' in [the second case]").

2.

Even assuming the issue of injury had been actually and essentially determined in *Hately I*—which it was not—the district court nevertheless erred in applying issue preclusion because Virginia continues to adhere to the doctrine of mutuality. *See Norfolk and Western Ry. Co. v. Bailey*, 272 S.E.2d 217, 219 (1980) (resisting the "modern trend" and choosing not to abrogate the mutuality requirement); *Scales*, 541 S.E.2d at 901 (requiring mutuality for defensive issue preclusion). That doctrine forbids a litigant from invoking issue preclusion "unless he would have been bound had the litigation of the issue in the prior action reached the opposite result." *Id.* (quoting *Angstadt*, 457 S.E.2d at 87). When a litigant "was not a party to the prior litigation, it would not have been bound had an opposite result been reached." *Angstadt*, 457 S.E.2d at 87 (citation omitted); *see Dual & Assoc., Inc. v. Wells*, 403 S.E.2d 354, 356 (Va. 1991) (holding that issue preclusion "cannot be asserted as a bar by a person who was a stranger to the prior litigation" (citation omitted)); *Ferebee v. Hungate*, 63 S.E.2d 761, 764 (Va. 1951) (holding that only a "party or privy" to a case would "have been prejudiced . . . had the decision been the other way").

In *Dual & Associates v. Wells*, a corporation filed two separate claims against a brother and a sister. 403 S.E.2d at 355. According to the corporation, the siblings

conspired to breach their fiduciary duties and to misappropriate corporate assets. *Id.* First, a trial court determined that the brother had not acted with "unclean hands" and that the brother was not liable. *Id.* The sister defensively asserted issue preclusion against the corporation and, thereafter, the trial court barred the corporation's claim. *Id.* at 356. The Supreme Court of Virginia reversed. Even though the corporation alleged that the siblings were co-conspirators, the sister "would not have been bound by a judgment entered in [favor of the corporation]." *Id.* Thus, the sister could not prove mutuality and therefore could not assert defensive issue preclusion. *Id.*

Similarly, in this case, Watts was dismissed from the *Hately I* action prior to Nicole's motion to dismiss the Virginia Computer Crimes Act claims. If Hately successfully demonstrated statutory injury in the *Hately I* action against Nicole, Watts nevertheless would have been given an opportunity to litigate the issue of injury in the current action. *See id* at 356; *Norfolk & W. Ry. Co.*, 272 S.E.2d at 219. Because Watts would not have been bound by the opposite result, the doctrine of mutuality precludes Watts from arguing that Hately's lack of injury was conclusively established in *Hately I*.

B.

As an independent basis for dismissing Hately's Virginia Computer Crimes Act claims, the district court held that Hately failed to plausibly allege statutory injury, therefore requiring dismissal under Federal Rule of Civil Procedure 12(b)(6). "We review de novo a district court's decision to dismiss for failure to state a claim, assuming all well-pleaded, nonconclusory factual allegations in the complaint to be true." *Aziz*, 658 F.3d at 391 (citations omitted). "To survive a motion to dismiss pursuant to Rule

12(b)(6), plaintiffs' factual allegations must be enough to raise a right to relief above the speculative level, thereby nudging their claims across the line from conceivable to plausible." *Id.* (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)) (alterations omitted). Although "a court must accept the material facts alleged in the complaint as true, statements of bare legal conclusions are not entitled to the assumption of truth and are insufficient to state a claim." *Id.* (citations and alterations omitted).

The Virginia Computer Crimes Act is a criminal statute with a private civil right of action. In pertinent part, the Virginia Computer Crimes Act provides: "Any person whose property or person is injured by reason of a violation of [the Virginia Computer Crimes Act] . . . may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, 'damages' shall include loss of profits." Va. Code Ann. § 18.2-152.12(A).

We previously have held that statutory injury under the Virginia Computer Crimes Act includes consequential damages. In *A.V. ex rel. Vanderhyne v. iParadigms, LLC*, a corporation sued a minor for obtaining access to its "service by using passwords and enrollment codes that [the minor] did not have authorization to use." 562 F.3d 630, 646–47 (4th Cir. 2009). Because the corporation was unaware of precisely how the minor had obtained access to its service, the corporation was forced to "assign[] several employees to determine what happened." *Id.* at 645. The corporation asserted that "over the course of about one week, numerous man-hours were spent responding to [the minor]'s use of the [service] password." *Id.* Based upon these facts, the district court granted summary judgment to the minor. Specifically, the district court determined that the corporation

"failed to present evidence of actual or economic damages" because these consequential damages did not fall within the meaning of the Virginia Computer Crimes Act. *Id.* at 647. We reversed. "Finding nothing in the statute to suggest that consequential damages are not available under [Virginia Computer Crimes Act, we held] that it was error to dismiss the [Virginia Computer Crimes Act] claim solely on this basis." *Id.*

Under *iParadigms*, Hately has pleaded facts that plausibly establish that he suffered consequential damages actionable under the Virginia Computer Crimes Act. In his operative complaint, Hately extensively details the time he spent assessing and rectifying Watts's unauthorized access. For example, Hately allegedly "identif[ied]" and "ma[de] several calls" to Blue Ridge College's technical support personnel "in order to ascertain the individual(s) that owns the domain for his school-related email account, as well as the individual(s) that manages the exchange servers for his school-related email account." J.A. 165 ¶ 94. Furthermore, Hately allegedly "review[ed]" "hundreds or thousands of email messages" and "restored" "deleted but unread email messages" that "were previously unknown to [Hately]." J.A. 166 ¶¶ 97–98. Finally, Hately allegedly "invested" time and money to "track and prevent future [unauthorized] access." J.A. 175 ¶ 153. The time Hately spent assessing and rectifying Watts's unauthorized access is materially indistinguishable from the time the corporation spent doing the same in *iParadigms*.

Watts seeks to avoid this plain application of *iParadigms* by suggesting that Hately has improperly valued his time spent assessing and rectifying the unauthorized access. But in considering a motion to dismiss, we assume "all well-pleaded,

nonconclusory factual allegations in the complaint to be true." *Aziz*, 658 F.3d at 391. Hately's "factual allegations" merely needed to "raise a right to relief above the speculative level, thereby nudging their claims across the line from conceivable to plausible." *Id.* (citing *Twombly*, 550 U.S. at 570) (alterations omitted). If Hately's alleged injuries are unsubstantiated, as Watts suggests, then these claims are appropriately dismissed at summary judgment—not under Rule 12(b)(6). *See OpenRisk, LLC, v. Microstrategy Servs. Corp.*, 876 F.3d 518, 528 (4th Cir. 2017), *cert. denied*, 138 S. Ct. 1575 (2018) (holding that district court properly awarded summary judgment on Virginia Computer Crimes Act claim in defendant's favor when plaintiff "failed to come forward with evidence of injury").

Here, Hately pleaded sufficient facts to make plausible his claim that he suffered injury under the Virginia Computer Crimes Act. Accordingly, the district court erred by dismissing Hately's Virginia Computer Crimes Act claims.

III.

Hately next contends that the district court erred in granting Watts summary judgment on Hately's Stored Communications Act claim. In particular, Hately argues that the court erred by concluding that "previously opened and delivered emails" stored "in a web-based email client" were not in protected "electronic storage" within the meaning of the Stored Communications Act. "We review the district court's grant of a motion for summary judgment de novo." *Nguyen v. CNA Corp.*, 44 F.3d 234, 236 (4th Cir. 1995) (citations omitted). Summary judgment is appropriate only when "there is no

genuine dispute as to an issue of material fact and the moving party is entitled to summary judgment as a matter of law." *Id.* at 236–37.

Before construing the meaning of the relevant statutory language, it is useful to recount Congress's purpose in enacting the Stored Communications Act. *See King v. Burwell*, 135 S. Ct. 2480, 2496 (2015) ("[A] fair reading of legislation demands a fair understanding of the legislative plan."). "Enacted in 1986, the Stored Communications Act was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails.'" *In re Google Inc. Cookie Placement Consumer Privacy Lit.*, 806 F.3d 125, 145 (3d Cir. 2015); (quoting *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 791 (5th Cir. 2012)); *see* H.R. Rep. No. 99-647, at 18 (1986); S. Rep. No. 99-541, at 2 (1986).

To Congress, this "legal uncertainty pose[d] potential problems in a number of areas." H.R. Rep. No. 99-647, at 19; *see* S. Rep. No. 99-541, at 5. First, it "unnecessarily discourage[d] potential customers from using innovative communications systems." S. Rep. No. 99-541, at 5; *see* H.R. Rep. No. 99-647, at 19. Next, it "encourage[d] unauthorized users to obtain access to communications to which they are not a party." S. Rep. No. 99-541, at 5; *see* H.R. Rep. No. 99-647, at 19. "Most importantly," Congress recognized that the uncertainty surrounding the legal protections, if any, afforded to electronic communications would "promote the gradual erosion of

th[e] precious right [to privacy]." S. Rep. No. 99-541, at 5; *see* H.R. Rep. No. 99-647, at 19.

Senator Patrick Leahy first introduced a bill to remedy this legal uncertainty in 1985. *See United States v. Councilman*, 418 F.3d 67, 76 (1st Cir. 2005) (en banc); S. Rep. No. 99-541, at 4. Shortly thereafter, the Congressional Office of Technology Assessment "released a long-awaited study on the privacy implications of electronic surveillance." *Councilman*, 418 F.3d at 76; S. Rep. No. 99-541, at 4. That report led to additional hearings and to the drafting of a new version of the bill, which Congress ultimately enacted. *See Councilman*, 418 F.3d at 77; S. Rep. No. 99-541, at 4.

In its report, the Office of Technology Assessment emphasized the lack of legal protection for email. The report, which the legislative history of the Stored Communications Act references at length, concluded that the "current legal protections for electronic mail are 'weak, ambiguous, or non-existent,' and that 'electronic mail remains legally as well as technically vulnerable to unauthorized surveillance.'" S. Rep. No. 99-541, at 4 (quoting Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 44 (Oct. 1985) ("*OTA Report*")). The report further identified the "stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver." *OTA Report*, at 45. Among the identified stages was the point at which the message was "in the electronic mailbox of the receiver." *Id.* Appreciating the legal uncertainty that existed, the report further noted that "electronic mail companies can reveal a great deal of information about an individual" and "[r]egardless of what [legal protection] the courts

may decide [to grant] based on the facts [of the] case, the issue requires [congressional] attention." *Id.* at 50.

Less than a year after the report was published, Congress enacted the Stored Communications Act. In so doing, Congress expressed its "judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004). The Stored Communications Act protects this interest in three principal ways. First, the Stored Communications Act limits the knowing disclosure of "electronic communications" by "electronic communication services" and "remote computing services." *See* 18 U.S.C. § 2702(a). Second, the statute circumscribes the government's power to compel the disclosure of electronic communications. *See* 18 U.S.C. § 2703. Third, the statute protects electronic communications from unauthorized access by third-parties. *See* 18 U.S.C. § 2701.

Section 2701 of the Stored Communications Act—under which Hately seeks relief—criminalizes and provides a private civil cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in *electronic storage* in such system[.]" 18 U.S.C. § 2701(a)(1) (emphasis added); *see also* 18 U.S.C. § 2707 (providing a civil cause of action). The Stored Communications Act defines "electronic storage" as follows:

> (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). The majority of courts have held—and we agree—that the two subsections recognize two discrete types of protected electronic storage. *See, e.g.*, *Theofel*, 359 F.3d at 1069; *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003), *as amended* (Jan. 20, 2004). That understanding conforms to the provision's legislative history, in which Congress stated that the definition of "electronic storage" encompasses "two types": (1) storage "incidental to transmission" and (2) "backup" storage. H.R. Rep. No. 99-647, at 68; *see also* S. Rep. 99-541, at 35 ("The term 'electronic storage' . . . includes *both* temporary, intermediate storage of a wire or electronic communication incidental to the transmission of the message, *and* any storage of such communication by the electronic communication service for purposes of backup protection of the communication." (emphases added)).

The district court concluded that Hately's emails that Watts allegedly accessed unlawfully—all of which the undisputed evidence establishes were previously delivered and opened—were not in "electronic storage" under either Subsection (A) or Subsection (B). *Hately*, 309 F. Supp. 3d at 410–14. Accordingly, we must interpret the Stored Communications Act to determine whether either Subsection (A) or Subsection (B) encompasses previously delivered and opened emails stored by a web-based email service.

"When interpreting a statute, we begin with the plain language." *In re Total Realty Mgmt., LLC*, 706 F.3d 245, 251 (4th Cir. 2013). In doing so, "we give the terms their ordinary, contemporary, common meaning, absent an indication Congress intended [it] to bear some different import." *Crespo v. Holder*, 631 F.3d 130, 133 (4th Cir. 2011) (citation omitted). "To determine a statute's plain meaning, we not only look to the language itself, but also 'the specific context in which the language is used, and the broader context of the statute as a whole.'" *In re Total Realty Mgmt.*, 706 F.3d at 251 (citation omitted). "If the plain language is unambiguous, we need look no further." *Lee v. Norfolk S. Ry. Co.*, 802 F.3d 626, 631 (4th Cir. 2015) (citation omitted). "On the other hand, if the text of a statute is ambiguous, we look to 'other indicia of congressional intent such as the legislative history' to interpret the statute." *Id.* (quoting *CGM, LLC v. BellSouth Telecomms., Inc.*, 664 F.3d 46, 53 (4th Cir.2011)).

A.

Whether Hately's previously opened and delivered emails stored by a web-based email service were in "electronic storage" within the meaning of Subsection (A) is a question of first impression in this Circuit. That provision encompasses "temporary, intermediate storage of a[n] . . . electronic communication incidental to the electronic transmission thereof[.]" 18 U.S.C. § 2510(17)(A).

Congress broadly defined "electronic communication" to include, with a few inapposite exceptions, "*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, photoelectric or photooptical system that affects interstate or foreign

commerce[.]" 18 U.S.C. § 2510(12) (emphasis added). The plain language of this definition encompasses email. And the legislative history confirms that Congress intended this definition to encompass email. *See* H.R. Rep. No. 99-647, at 34 (recognizing that the definition of "electronic communications" provides "electronic mail" "with protection against interception"); S. Rep. No. 99-541, at 14. Thus, email is a form of "electronic communication" within the meaning of the Stored Communications Act.

Numerous courts have reached the same conclusion. *See, e.g., Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 964 (11th Cir. 2016) (recognizing that emails are "subject to the protections of 18 U.S.C. § 2701(a)"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) (recognizing that Congress intended for the Stored Communications Act to "protect electronic communications that are configured to be private, such as email"); *In Matter of App. of U.S. for an Order Authorizing the Installation & Use of a Pen Register & a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 16 (D.D.C. 2006) ("Given that the statute defines an electronic communication to be any 'transfer of signals' of 'any nature' by means of virtually any type of transmission system (*e.g.*, wire, electromagnetic, etc.), there can be no doubt it is broad enough to encompass e-mail communications and other similar signals transmitted over the Internet.").

Even so, the district court held that previously delivered and opened emails—like Hately's emails at issue—"are no longer in 'temporary, intermediate storage . . . incidental to the[ir] electronic transmission'" and therefore do not fall within the scope of Subsection (A). *Hately*, 309 F. Supp. 3d at 410. We agree.

Dictionaries define "temporary" as "existing or continuing for a limited time," *Temporary*, Webster's Third New International Dictionary 2353 (1961), and "intermediate" as "lying or being in the middle[,]" *Intermediate*, Webster's Third New International Dictionary 1180; *see also* The American Heritage Dictionary 914, 1781 (4th ed. 2000) (defining "temporary" as "lasting, used, serving, or enjoyed for a limited time" and "intermediate" as "lying or occurring between two extremes or in a middle position or state"). These definitions indicate that electronic communications are protected by Subsection (A) while they are stored "for a limited time" "in the middle" of transmission. *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001).

But previously opened and delivered emails stored by a web-based email service do not fall within the plain language of Subsection (A). Such emails already have been "transmitted" to the recipient and therefore no longer are "in the middle" of transmission. *See Councilman*, 418 F.3d at 81 (holding that Subsection (A) "refers to temporary storage, such as when a message sits in an email user's mailbox after transmission but before the user has retrieved the message from the mail server"); *Theofel*, 359 F.3d at 1075; *Fraser*, 352 F.3d at 114 (holding that an email in "post-transmission storage" was "not in temporary, intermediate storage"). Likewise, a recipient's decision not to delete an email after receiving and opening the message suggests that the recipient does not intend to keep the message for a "limited" amount of time. *See infra* Part III.B.4. Thus,

previously received and accessed emails are in not protected "electronic storage" under Subsection (A).[4]

B.

In the alternative, Hately contends that previously opened and delivered emails stored in a web-based email client are in "electronic storage" within the meaning of Subsection (B), which encompasses "any [1] storage of [2] such communication [3] by an electronic communication service [4] for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B). This too is a question of first impression in this Circuit. As further explained below, we conclude that previously opened and delivered emails fall within each element of this definition.

1.

To be in protected "electronic storage" under Subsection (B), previously opened and delivered emails must be in "storage." *See* 18 U.S.C. § 2510(17)(B). Ordinarily, something is "stored" when it is "reserved for future use." *Store*, The American Heritage Dictionary 1708; *see also Store*, Webster's Third New International Dictionary 2252 ("[T]o record (information) in an electronic device (as a computer) from which the data can be obtained as needed."). Congress indicated it intended for courts to construe the

[4] During the email transmission process, intermediate computers may "retain backup copies, which they delete later." *Councilman*, 418 F.3d at 70. We do not decide whether Subsection (A) protects copies of email messages made and stored "in the middle of transmission," which copies continue to remain in storage *after* the recipient receives and opens a separate copy of the email message in his email client.

meaning of "storage" broadly, stating that it did not intend to limit the term to particular mediums, forms, or locations. *See* H.R. Rep. No. 99-647, at 39.

In light of the ordinary meaning of storage and Congress's intent that the term be interpreted broadly, we agree with the Ninth Circuit that "prior access is irrelevant" to whether an email is in "storage," *Theofel*, 359 F.3d at 1077—*i.e.*, "reserved for future use" or available to "be obtained as needed." When a user of a web-based email client, like Hately, opens a message and then chooses not to delete the message after he reads it, the message remains "reserved" on the host server for "future use"—*i.e.*, in the event the user needs to view the message again. *See id.* at 1075; *accord Cheng v. Romo*, No. CIV.A. 11-10007-DJC, 2013 WL 6814691, at *4 (D. Mass. Dec. 20, 2013) (holding that copies of delivered and opened emails accessed through a web-based email client were in "storage" for purpose of Subsection (B)); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) ("[T]he majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider's systems after it has been delivered . . . is a stored communication subject to the [Stored Communications Act]."); *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156, at *5–6 (E.D. Mich. Feb. 6, 2008) ("The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.").

Regardless of whether Hately had previously opened and accessed his web-based emails, those emails were nevertheless "reserved for future use" by the Blue Ridge

College email host in the event that Hately would need to access them in the future. Accordingly, Hately's emails were in "storage" within the meaning of Subsection (B).

2.

Next, to be in protected "electronic storage" under Subsection (B), previously opened and delivered emails must be included within the meaning of the phrase "such communication." *See* 18 U.S.C. § 2510(17)(B). The phrase "such communication" relates back to Subsection (A), which provides: "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

Watts argues—and the district court agreed—that to fall under Subsection (B) a "communication" must be both "wire or electronic" *and* in "temporary, intermediate storage" because both of those phrases precede the term "communication" in Subsection (A). *Hately*, 309 F. Supp. 3d at 413 ("'[S]uch communication' in § 2510(17)(B) refers to communication 'temporar[ily and] intermediate[ly]' stored 'incidental to the electronic transmission thereof."). By contrast, Hately contends that Congress intended the term "such" in Subsection (B) to serve as a shorthand for the phrase "wire or electronic" in Subsection (A). We agree with Hately.

As the Ninth Circuit explained, "Subsection (A) identifies a type of communication ('a wire or electronic communication') *and* a type of storage ('temporary, intermediate storage . . . incidental to the electronic transmission thereof')." *Theofel*, 359 F.3d at 1076 (emphasis added). "The phrase 'such communication' in [S]ubsection (B) does not, as a matter of grammar, reference attributes of the type of *storage* defined in subsection (A)." *Id.* (emphasis added). Put simply, the phrase "temporary, intermediate"

modifies the noun "storage," but does not modify the noun "communication"—the term referred to in Subsection (B). Therefore, "as the statute is written, 'such communication' is nothing more than shorthand for 'a wire or electronic communication." *Id.*; *accord Bailey*, 2008 WL 324156, at *6 ("The phrase 'such communication' in [Subsection (B)] refers to 'wire or electronic communications' as mentioned in [Subsection (A)].").

Our interpretation also conforms to the principle of statutory construction that "if possible, a court should avoid an interpretation that renders any 'clause, sentence, or word . . . superfluous, void, or insignificant.'" *Clark v. Absolute Collection Serv., Inc.*, 741 F.3d 487, 491 (4th Cir. 2014) (citing *Duncan v. Walker*, 533 U.S. 167, 174 (2001)); *see Freeman v. Quicken Loans, Inc.*, 566 U.S. 624, 635 (2012). Were we to construe "such communication" as encompassing only wire or electronic communications in "temporary, intermediate storage," Subsection (B) would be rendered "essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary, intermediate storage' within the meaning of [S]ubsection (A)." *Theofel*, 359 F.3d at 1075–76.

Hately's emails constitute "wire or electronic communication" as the Stored Communications Act uses that term. *See supra* Part III.A. Accordingly, the district court erred in holding that Hately's emails did not constitute "such communication" within the meaning of Subsection (B).

3.

Third, to constitute "electronic storage" for purposes of Subsection (B), the wire or electronic communication must be stored by an "electronic communication service." 18

U.S.C. § 2510(17)(B). The Stored Communications Act defines "electronic communication service," as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15). As explained above, email is a form of "electronic communication" for purposes of the Stored Communications Act. *See supra* Part III.A. Under the plain language of Section 2510(17)(B), therefore, "any service which provides to users thereof the ability to send or receive" email messages constitutes an electronic communication service. Because Blue Ridge College's email service enables account holders, like Hately, to "send or receive" email messages, it falls within the plain language of the Stored Communications Act's definition of electronic communication service.

Notably, the Stored Communications Act's legislative history supports this conclusion, stating that "electronic mail companies are providers of electronic communication services." S. Rep. No. 99-541, at 14. And in accordance with the plain language of the Stored Communications Act and the statute's legislative history, courts have concluded that email services—like Hately's College email account—are electronic communication services. *See, e.g.*, *Vista Mktg.*, 812 F.3d at 963–64 (holding that the defendant "qualified as an [electronic communication service] because it was a service that provided [the plaintiff's] employees with the ability to send and receive electronic communications, including emails."); *Warshak v. United States*, 532 F.3d 521, 523 (6th Cir. 2008) (holding that the definition of electronic communication service "covers basic e-mail services"); *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 901 (9th Cir. 2008), *rev'd on other grounds*, *City of Ontario, Cal. v. Quon* (2010) (holding that "a

provider of e-mail services [is] undisputedly an [electronic communication service]"); *In re United States for an Order Pursuant to 18 U.S.C. § 2705(b)*, 289 F. Supp. 3d 201, 208 (D.D.C. 2018) (holding that online booking company was an electronic communication service for purposes of dispute related to disclosure of messages in the company's "user-to-user electronic messaging system").

Watts nevertheless argues—and the district court agreed—that, at least for purposes of the email copies in question, Blue Ridge College's email service was functioning not as an electronic communication service, but *solely* as a "remote computing service"—a term not used in the Stored Communications Act's definition of electronic storage. The Stored Communications Act defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). According to the district court, Blue Ridge College's email service "was not acting as an [electronic communication service] with respect to" the copies of Hately's "delivered and opened" emails accessed by Watts but was instead providing "storage or processing" of the emails, and therefore was acting as a remote computing service. *Hately*, 309 F. Supp. 3d at 413.

The district court's reasoning rests on the premise that, for purposes of the emails in question, Blue Ridge College's email service could not simultaneously function as *both* an electronic communication service *and* a remote computing service. But nothing in the plain language of the definitions of electronic communication service and remote computing service precludes an entity from simultaneously functioning as both. There is

no logical or technological obstacle to an entity "provid[ing] to users thereof the ability to send or receive wire or electronic communications"—*i.e.*, functioning as an electronic communication service—*while*, and as part of the same service, "provi[ding] the public [with] computer storage or processing services by means of an electronic communications system"—*i.e.*, functioning as a remote computing service. And the relevant legislative history expressly contemplates as much, stating that "remote computing services may also provide electronic communication services." S. Rep. No. 99-541, at 14; *see also* H.R. Rep. No. 99-647, at 64 ("[T]o the extent that a remote computing service is provided through an Electronic Communication Service, then such service is also protected [under Section 2701(a)].").

Notably, other aspects of the district court's opinion appear to contradict its conclusion that an entity cannot simultaneously function as an electronic communication service and a remote computing service. In particular, the district court held—and Watts does not dispute—that the email provider was acting as an electronic communication service as to unread or not downloaded emails. *See Hately*, 309 F. Supp. 3d at 413 ("[P]aragraph (B) refers to a copy of a communication, *made by the* [*electronic communication service*] while the communication was in transit[.]" (emphasis added)); *see also id.* ("[O]nce an email has been delivered and opened, its transmission is complete, the [electronic communication service] is *no longer* storing it 'incident to transmission.'" (emphasis added)). When, as here, emails are accessed through a web-based email service, then the provider of the email service necessarily would, under the district court's reasoning, also seem to be providing "remote computing services" as to

"unread or not downloaded" emails because it is providing "storage . . . by means of an electronic communications system." 18 U.S.C. § 2711(2).

The legislative history also supports the conclusion that Congress viewed email providers as simultaneously functioning as both a remote computing service and an electronic communication service when such providers store "unread or not downloaded" messages. The House Report notes that "[s]ometimes the addressee, having requested and received a message, chooses to leave it in storage on the [remote computing] service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should *continue to be covered* by section 2702(a)(2)," which prohibits *remote computing services* from divulging the contents of communications they carry or maintain. H.R. Rep. No. 99-647, at 64–65 (emphasis added). If a provision protecting messages stored by remote computing services "applies to e-mail *even before access*, the committee could not have been identifying an *exclusive* source of protection, since . . . unopened e-mail is protected by the electronic storage provisions." *Theofel*, 359 F.3d at 1070 (emphases added).

Significantly, because the plain language of the Stored Communications Act, the statute's legislative history, and the district court's own reasoning contemplates that entities can simultaneously function as both an electronic communication service and a remote computing service, the House Report's statement that a user's opened messages "continue to be covered" by remote computing service provisions in no way precludes a finding that the entity also "continue[d] to" act as an electronic communication service

after the user opened the messages. *See id.* (stating that because the House Report's statement "addresses provisions relating to remote computing services[,] [w]e do not read it to address whether electronic storage provisions also apply"). And because an entity can simultaneously function as an electronic communication service and a remote computing service, an entity's status as a remote computing service in no way precludes a determination that the entity also was acting as an electronic communication service.[5]

---

[5] One commentator has argued, and some courts have agreed, that an email cannot "be protected under the [electronic communication service] rules and the [remote computing service] rules at the same time" because "the [electronic communication service] rules and [remote computing service] rules can be mutually exclusive." 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); *see also, e.g.*, *Am. Health, Inc. v. Chevere*, Civ. No. 12-1678, 2017 WL 6561156, at *8 n.4 (D.P.R. Dec. 22, 2017). Kerr reasons that the electronic communication service rules and remote computing service rules are "mutually exclusive" because "§ 2703(a) states that a government entity needs a warrant to compel a service provider acting as an [electronic communication service] to disclose contents so long as the contents have been in storage for 180 days or less" whereas "§ 2703(b)(1)(B)(i) states that the government entity can compel a service provider acting as [a remote computing service] to disclose contents with only prior notice." *Id.* "If an email message is covered by both the [electronic communication service] and [remote computing service] rules at the same time, legal process that is permitted under the [remote computing service] rules would violate the [electronic communication service] rules," he reasons. *Id.*

There are several problems with this analysis. To begin, because both Section 2703(a) and Section 2703(b)(1)(B)(i) can be satisfied at the same time—by, for example, obtaining a warrant, § 2703(b)(1)(A)—they are not "mutually exclusive" in the logical sense. *See Mutually Exclusive*, Merriam-Webster.com (last visited Feb. 26, 2019) (defining "mutually exclusive" as "being related such that each excludes or precludes the other").

More significantly, both the House Report and Senate Report recognize that there are instances "in which a person or entity acts both as a provider of [electronic communications] services and also offers other services to the public," which other services may be subject to different statutory disclosure requirements. H.R. Rep. No. 99-
(Continued)

To be sure, "the statutory definitions of [electronic communication service] and [remote computing service] are functional and context sensitive." *In re United States*, 289 F. Supp. 3d at 210. Therefore, an entity that acts as an electronic communication service in one context may act as *only* a remote computing service in another context or, in still other contexts, may *not* act as either an electronic communication service or a remoting computing service. *Id.* For example, we conclude today that companies such as Microsoft and Google function as an electronic communication services when they provide email services through their proprietary web-based email applications. But that does not mean that Microsoft and Google necessarily function as electronic communication services regarding other applications and services they offer, like cloud-based data processing and analytics services, or goods or products they sell or license, like hardware or software.

Because (1) email providers fall squarely within the statutory definition of electronic communication service and (2) the terms electronic communication service and

---

647, at 65; S. Rep. No. 99-541, at 37. Congress stated that in such circumstances, the provider should adhere to the more restrictive disclosure regime. H.R. Rep. No. 99-647, at 65 ("The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure."); S. Rep. No. 99-541, at 37 (same). For example, Congress stated when an entity simultaneously is subject to both the remote computing service and the Fair Credit Reporting Act disclosure restrictions, the entity should adhere to the more onerous Fair Credit Reporting Act disclosure restrictions. H.R. Rep. No. 99-647, at 65. Applying Congress's intended analytical approach, entities that simultaneously function as an electronic communication service and a remote computing service would follow the more restrictive disclosure regime set forth in Section 2703(a).

remote computing service are not mutually exclusive, the district court erred in holding Hately's College email account did not amount to an electronic communication service.

4.

Finally, to constitute "electronic storage" under Subsection (B), an electronic communication must be stored "for purposes of backup protection." 18 U.S.C. § 2510(17)(B). Notwithstanding that the Stored Communications Act defines numerous terms, the statute does not define the term "backup protection." Accordingly, we must look to the term's plain meaning and Congress's intent in enacting the Stored Communications Act and Section 2701(a), in particular, to determine whether previously delivered and opened emails stored by a web-based email service are stored for "purposes of backup protection."[6]

The most relevant definition of "backup" is "a *copy* of computer data (such as a file or the contents of a hard drive)." *Backup*, Merriam-Webster.com (last visited Feb.

[6] Although no Circuit court appears to have squarely addressed the question, courts are divided as to whether delivered and previously opened emails retained on the server of the host of a web-based email service are stored for "purposes of backup protection." Several courts, including the district court in this case, have concluded that such emails cannot amount to "backup[s]" because the term "backup" presupposes the existence of another copy to which this e-mail would serve as a substitute or support. *See Hately*, 309 F. Supp. 3d at 413 n.9; *Jennings*, 736 S.E.2d at 245 (noting that "[t]he ordinary meaning of the word 'backup' is 'one that serves as a substitute or support'"); *see also*, *e.g.*, *Cobra Pipeline Co., Ltd. v. Gas Natural, Inc.*, 132 F. Supp. 3d 945, 952 (N.D. Ohio 2015) (holding that term "stored for backup purposes" does not encompass "primary" copies). Other courts have concluded that previously opened emails retained on the server of the host of a web-based email service constitute wire or electronic communications stored for the purposes of backup protection. *See, e.g.*, *Cheng*, 2013 WL 6814691, at *5–7; *Pure Power*, 587 F. Supp. 2d at 555–56.

26, 2019) (emphasis added). A "copy" is a "duplicate." *Copy*, Merriam-Webster.com (last visited Feb. 26, 2019); *Copy*, The American Heritage Dictionary 405. More general definitions of "backup" include "substitute" or "support." *Backup*, Merriam-Webster.com (last visited Feb. 26, 2019); *Backup*, The American Heritage Dictionary 132. "Protection" is defined as "the act of protecting," *Protection*, Merriam-Webster.com (last visited Feb. 26, 2019), which means "cover[ing] or shield[ing] from exposure, injury, damage, or destruction," *Protect*, Merriam-Webster.com (last visited Feb. 26, 2019); *see also* The American Heritage Dictionary 1408 (defining "protect" as "to keep from being damaged, attacked, stolen, or injured"). Accordingly, a wire or electronic communication is stored for "purposes of backup protection" if it is a "copy" or "duplicate" of the communication stored to prevent, among other things, its "destruction."

The copies of previously delivered and opened emails retained on the server of the host of a web-based email service—like Hately's emails at issue—fall within this understanding of electronic communication stored "for purposes of backup protection." To understand why such emails fall within the definition of "*backup*," it is useful to explain the typical manner in which a web-based email service functions.

To begin, after the sender drafts and sends a message, a copy of the message is transmitted to the recipient's web-based email service. Such services typically (including Google, which hosted Blue Ridge College's email service) "utilize completely redundant systems consisting of multiple data servers." *See* Br. of Amici Curiae the Ctr. for Dem. & Tech., the Elec. Frontier Found., and New Am. Open Tech. Inst. in Support of Pl.-

Appellant and Reversal ("CDT Br.") at 22. "In redundant systems, a single email is stored on multiple servers, likely in different locations around the country, and possibly around the world." *Id.* Web-based email services store copies of messages on multiple servers in order "to decrease email downtime (*i.e.*, users being unable to access their email) or loss of information" in the event any one server fails. *Id.* Accordingly, when a web-based email service receives an email, it typically generates numerous copies of the email, the existence of which ensures that the inaccessibility or failure of a particular server or the errant destruction of any one copy will not lead to the loss of a message. Put differently, in a web-based email service, each "copy" serves as a "substitute" or "support" for the many other copies stored by the service. *See id.; see also Reliability*, Google Cloud Support, https://support.google.com/googlecloud/answer/6056635?hl=en (last visited Feb. 26, 2019) ("[A]ll Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of a machine failure, data will still be accessible through another system."); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. Telecomm. & High Tech. L. 359, 361 (2010) ("Cloud computing services provide consumers with vast amounts of cheap, redundant storage and allow them to instantly access their data from a web-connected computer anywhere in the world.").

When the recipient chooses to view the email via a web browser or application on a computer, smartphone, or other internet-connected device, one of the web-based email

service's servers sends a copy of the message to the user's device for the user to view through the browser or application. That copy is temporarily stored in the device's short-term memory. The user's device also might download a copy for retention in the device's long-term memory. Accordingly, the "copies" retained by the host of the web-based email service also serve as a "substitute" or "support" for the copies of the message the recipient downloads to his device's short-term or long-term memory. *Accord Cheng*, 2013 WL 6814691, at *3 ("[R]egardless of the number of times [the plaintiff] or [the defendant] viewed [the plaintiff's] email (by downloading web page representations of those emails into their person computer's web browser) the Yahoo! server continued to store copies of those same emails that previously had been transmitted to [the plaintiff's] web browsers, and again to [the defendant's] web browser.").

Numerous other copies may exist as well. For example, the sender may retain a copy of the message in her outbox. The sender's email service also may retain copies of the message on one or more servers for the sender to access. And during the transmission process, intermediate computers may retain one or more copies as well. *See Councilman*, 418 F.3d at 70.

Notably, notwithstanding that some courts have lamented that "[i]t is not always easy to square the decades-old [Stored Communications Act] with the current state of email technology," *see, e.g.*, *Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 839 n.5 (8th Cir. 2015), the way modern web-based email services function is closely analogous to how Congress described the "most common form" of email used at the time it enacted the Stored Communications Act: "[M]essages are typed into a

computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer 'mail box' until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer." S. Rep. No. 99-541, at 8. Just as in the system Congress described, in a modern web-based email service, a sender's email service transmits a message to the addressee's web-based email service. Also like the system Congress described, the web-based email service then "stores" the message until the addressee "retrieves" it, by routing the message through the addressee's internet provider to the browser or application on the addressee's internet-connected device in which the addressee views the message.[7]

The copies of emails retained by a user in his web-based account also are stored by the web-based email service—*i.e.*, the electronic communication service—for purposes of its own and its users' "protection." As set forth above, web-based email services—including Google, which hosted the copies Hately's emails accessed by Watts—retain multiple copies of the messages in a user's account for the web-based email service's *own* backup protection. Such services use "redundant" systems "to

[7] That modern web-based email systems typically download messages to short-term memory as opposed to long-term storage does not render Congress' exemplar email system any less relevant. Congress intended for the term storage to be defined broadly, stating that the meaning of storage should not be limited to particular mediums, forms, or locations. *See supra* Part III.B.1. Accordingly, changes in the manner or medium of storage do not impact whether an electronic communication falls within the definition of electronic storage.

decrease email downtime (*i.e.*, users being unable to access their email) or loss of information due to component failure," CDT Br. at 22—*i.e.*, to ensure the product the web-based email service markets functions as intended, expected, and demanded by users. Put simply, by storing copies of messages on multiple servers and in multiple locations, the web-based email service protects itself against the failure of one or more of its servers.

Additionally, the web-based email service stores previously opened and delivered emails for the "protection" of their users. When the user of a web-based email service, like Hately, opens and reviews an email message and then chooses not to delete the message from his account, the user is likely retaining that message to prevent its destruction. There are numerous reasons a recipient may not want to destroy a message he already has read. For example, a user who receives an email setting up a meeting may choose not to delete the email after first reading it because the user wants to keep a copy readily available in case the user forgets the time or place of the meeting. Or, a user who reaches a business agreement over email may choose to retain in his web-based account messages concerning the agreement to document the agreement's existence and terms. Or, a user who receives a message from a friend or loved one may choose not to delete the message because it has sentimental value and the user wishes to reread the message of future. Or, a user may choose not to delete a message after reading it simply because the user does not know whether the user will need the message in the future and therefore wishes to preserve it. In each of these examples, the user chooses not to delete the message because the user does not want the message to be "destroyed."

But importantly, the meaning of "backup protection" does not turn on whether a *user* subjectively chose not to delete the email after reading the message because the *user* wanted to keep the message for backup protection. That is because the purpose of the *web-based email service* in providing storage for the message—storage that is a feature of the product the web-based email service offers—is to afford the user a place to store messages the user does not want destroyed. The *web-based email service* does not need to know why the user has elected not to delete particular message. Rather, the *web-based email service* recognizes that users who choose to use a web-based email platform desire storage for read and unread messages and therefore the *web-based email service* provides such storage to meet user demand. That is why providers of web-based email services like Google, Microsoft, and Yahoo! market the amount of storage their services provide. *See, e.g.*, Nicholas Behrens, *Gmail, now with 10 GB of Storage (and counting)*, Official Gmail Blog (April 24, 2012), https://gmail.googleblog.com/2012/04/gmail-now-with-10-gb-of-storage-and.html (last visited Feb. 26, 2019). Put simply, the *web-based email service* is storing the message for the purpose of providing backup protection to its users because that is a feature users desire.

Our conclusion that previously delivered and opened emails stored on a web-based email client are in "electronic storage"—and therefore actionable under Section 2701(a)—also finds support in the statute's legislative history. The House Report states that "[a]n 'electronic mail' service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701." H.R. Rep. No. 99-647, at 63. In the case of a web-based

email service, like Blue Ridge College's email service, the service holds copies of the message in "storage" on one or more of its servers "until the addressee requests it." *Id.* Notably, in the case of a web-based email service—like Blue Ridge College's email service—an addressee can "request" a message on multiple occasions—*i.e.*, each time the addressee elects to open the message in his web-based email client, regardless of whether the addressee previously opened the message. Nothing in the House Report indicates that Congress intended to limit Section 2701's protections to the period before the addressee *first* requests a message—as Watts argues.

Likewise, the Senate Report notes that "a computer mail facility authorizes a subscriber to access information in their portion of the facilit[y']s storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of [Section 2701(a)]." S. Rep. No. 99-541, at 36. Here, Google, as host of Blue Ridge College's email service, allocates a "portion" of the space on its servers to store a user's messages. Accordingly, accessing that "storage . . . without specific authorization"—as Watts allegedly did here—is actionable under Section 2701(a)(1). Again, the Senate Report nowhere draws a distinction between the periods before and after a user first views a message, as Watts would have us do. Rather, like the House Report, the Senate Report focuses on whether the copy of the allegedly unlawfully accessed message was held in the web-based email service's storage (and therefore is actionable under Section 2701(a)(1)) as opposed to other entities' storage (and therefore is not actionable).

Watts nevertheless argues that previously delivered and opened emails stored by a web-based email service do not fall within the meaning of "backup protection" for three

reasons: (1) the term encompasses only copies "made for the service provider's own administrative purposes"; (2) the term encompasses only copies retained "for use in the event that the *original* is rendered unusable"; and (3) the emails were stored for *Hately*'s backup protection and not for *Blue Ridge College*'s backup protection.

Watts' first argument—that the term "backup protection" encompasses only copies "made for the service provider's own administrative purposes"—principally rests on his contention, with which the district court agreed, that the meaning of "backup protection" in Subsection (B) should be construed in accordance with the meaning of "backup copy" in 18 U.S.C. § 2704. *See Hately*, 309 F. Supp. 3d at 413 n.9 (quoting Kerr, *supra*, at 1217 n.61 ("Section 2704 makes clear that the Stored Communications Act uses the phrase 'backup copy' in a very technical way to mean a copy made by the service provider for administrative purposes.")). Section 2704 provides that the government "may include in its subpoena or court order [requesting communications stored by a remote computing service] a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve the communications." Accordingly, the term "backup copy" in Section 2704 means a copy of an electronic communication created by a service provider pursuant to a court order.

Section 2704's use of the term "backup copy" does not bear the interpretive weight Watts claims. Nothing in the Stored Communications Act's definition of electronic storage, Section 2704, or the statute's legislative history provides any indication that Congress intended "backup protection" and "backup copy" to have the

same meaning. On the contrary, Section 2704(a) deals with a specific type of "backup copy"—one created pursuant to court order—and therefore does not, and cannot, establish the general definition of "backup." Notably, Watts and the district court concede as much, concluding that the definition of "backup protection" encompasses all "backup" copies created for an electronic communication service's "administrative purposes," not just any backup copies created pursuant to a court order issued under Section 2704(a). Indeed, the "backup copies" at issue in Section 2704(a) arguably are not created for "administrative purposes" at all—they are created to comply with the court order.

More significantly, even assuming Watts and the district court are correct that the term "backup protection" encompasses only copies that are "made for the service provider's own administrative purposes," Hately's emails in question would fall within the meaning of "backup protection." "Administrative" means "relating to the running of a business, organization, etc." *Administrative*, Merriam-Webster.com (last visited Feb. 26, 2019). As explained above, web-based email services—including Google, which hosted Hately's College email account—create numerous copies of emails for their own administrative purposes, such as decreasing email downtime, protecting against loss of data in the event a particular server fails, CDT Br. at 22, and for their own commercial purposes, such as to more effectively target advertisements. Accordingly, the copies of Hately's emails at issue were created for Blue Ridge College email service's "administrative purposes" under the common meaning of that term.

In support of his second argument—that the term "backup protection" encompasses only copies retained "for use in the event that the *original* is rendered unusable"—Watts asserts that the definition of backup presupposes the existence of an "original." Appellee's Br. at 33–34; *see also Jennings*, 736 S.E.2d at 245 ("Congress's use of 'backup' necessarily presupposes the existence of another copy to which this e-mail would serve as a substitute or support."). According to Watts, the emails accessed by users of a web-based email service are "originals," rather than "copies," and therefore do not fall within the meaning of "backup."

To be sure, some definitions of "backup" suggest a distinction between "backups" and "originals." *See Backup*, The American Heritage Dictionary 132 ("A copy of a program or file that is stored separately from the original."); *Copy*, The American Heritage Dictionary 405 (defining "copy" as "[a]n imitation or reproduction of an original"). But not all definitions of "backup" draw such a distinction. *See supra* Part III.B.4. And relying on definitions of "backup" that define the term relative to an "original" makes little sense in the context of messages stored by electronic communication services, and email services, in particular. That is because the "original" would seem to be most readily understood as the copy of a message that a *sender* types into his email client. The sender's email service then sends a copy of that original to the recipient's email service, meaning that the recipient's email service never receives, much less stores, the "original" message. *See* S. Rep. No. 99-541, at 8 (stating that in the "most common form" of email "messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail

company. If the intended addressee subscribes to the service, the message is stored by the company's computer 'mail box' until the subscriber calls the company to retrieve its mail"). Put differently, all copies of an email held by a recipient's email service, web-based or otherwise, are "copies," rather than "originals."

Additionally, even if an addressee's email service did receive an "original," in the context of "redundant" web-based email services—like Blue Ridge College's email service hosted by Google—even the "original" serves as a "backup." *See* CDT Br. at 22. In particular, each of the numerous copies of the messages created and stored on the service's server acts as a "substitute" or "support" for every other copy stored on the service's servers. *See id.* Accordingly, even if one of those numerous copies was an "original," that "original" would still serve as a "backup" for all the other copies stored by the service.[8]

[8] Although the district court did not accept Watts' effort to distinguish "backup" copies from "original" copies, in defining backup the district court did distinguish between (1) Blue Ridge College's "storage copies" of the emails, which were accessible to the student only "by special request," and (2) Blue Ridge College's "service copies" of the emails, which were "immediately accessible to the user by logging in to the email client." *Id.* at 411–12. According to the district court, the Stored Communications Act protects only "storage copies." *Id.* Because Watts accessed "service," rather than "storage," copies of Hately's emails, Hately cannot obtain relief under the Stored Communications Act, the district court determined. *Id.* We reject this distinction for several reasons.

To begin, neither Subsection (B), nor the Stored Communications Act overall, nor the statute's legislative history uses the terms "storage copies" or "service copies." Accordingly, the district court's analytical framework lacks textual support. Additionally, that Blue Ridge College maintained "storage copies"—as the district court defined that term—of emails for backup protection in no way precludes a determination that "service copies" also are "stored for purposes of backup protection," as Congress (Continued)

Third, Watts argues—and the district court agreed—that Hately's emails were not stored "for purposes of backup protection" because the court determined those emails were stored for *Hately*'s backup protection and not for *Blue Ridge College email service*'s backup protection. *See Hately*, 309 F. Supp. 3d at 413 (holding that Subsection (B) "refers to a copy of a communication . . . stored by the [electronic communication service] for its *own* backup or administrative purposes" (emphasis added)). But, as explained above, messages stored by a web-based email service are stored for purposes of the web-based email service's own backup protection as well as the user's backup protection. Equally important, "nothing in the [Stored Communications Act] requires that the backup protection be for the benefit of the [electronic communication service] rather than the user." *Theofel*, 359 F.3d at 1075. On the contrary, the statute's legislative history expressly contemplates that the requisite backup protection may be for the benefit of the user. H.R. No. 99-647, at 68 ("Back up protection preserves the integrity of the electronic communication system and to some extent *preserves the property of the users of such a system*." (emphasis added)).

* * * * *

---

used that term. Neither the statute nor its legislative history limits the scope of messages in "electronic storage" under Subsection (B) to a single backup copy or type of backup copy. On the contrary, as long as Blue Ridge College's email service stored the "service copies" of Hately's emails "for purposes of backup protection" as required by Subsection (B), it is irrelevant that additional backup copies—be they characterized "storage copies" or otherwise—also may exist.

We conclude that previously delivered and opened emails stored by an electronic communication service are stored for "purposes of backup protection," under the plain and ordinary meaning of those terms. And because such emails amount to "wire or electronic communications" in "storage" by an "electronic communication service," such emails are in "electronic storage" for purposes of Subsection (B). *See supra* Parts III.B.1–3.[9]

5.

Our conclusion that previously delivered and opened emails fall within the meaning of Subsection (B) also accords with Congress's purpose in enacting the Stored Communications Act. Congress sought to fill in a "gap" in then-existing law as to the "protect[ion of] the privacy and security of communications transmitted by new non-common carrier communications services or new forms of telecommunications and computer technology," including email. S. Rep. No. 99-541, at 5; H.R. Rep. No. 99-647, at 17 (noting that statutory framework that existed prior to enactment of the Stored Communications Act "appear[ed] to leave unprotected an important sector of the new communications technologies," including email); *id.* at 18 (noting "[t]he statutory

[9] Watts also asserts that language in the legislative history of two bills considered by Congress more than a decade *after* it enacted the Stored Communications Act establishes "Congress's intent that opened and retained emails not be considered in 'electronic storage.'" Appellee's Br. at 45. But "the interpretation given by one Congress (or a committee or Member thereof) to an earlier statute is of little assistance in discerning the meaning of that statute." *Pub. Employees Ret. Sys. of Ohio v. Betts*, 492 U.S. 158, 168 (1989). Accordingly, we decline to rely on subsequent legislative history as a basis to ignore the Stored Communications Act's plain meaning and *its* legislative history.

deficiency . . . with respect to non-voice communications"). As noted above, Congress expressed concern that the absence of such protection "unnecessarily discourage[s] potential customers from using innovative communications systems" and "encourages unauthorized users to obtain access to communications to which they are not a party." S. Rep. No. 99-541, at 5; H.R. Rep. No. 99-647, at 19.

The district court's construction of Subsection (B)—that previously delivered and opened emails stored by a web-based email service are not in "electronic storage" and therefore not actionable under Section 2701(a)(1)—would materially undermine these objectives. Potential users of web-based-email services—like Blue Ridge College's email service—would be deterred from using such services, knowing that unauthorized individuals and entities could access many, if not most, of the users' most sensitive emails without running afoul of federal law. Likewise, without the prospect of liability under federal law, unauthorized entities will face minimal adverse consequences for accessing, and using for their own benefit, communications to which they are not a party. The legislative history establishes that Congress did not intend such a result.

The district court's interpretation of Subsection (B)—which would protect only *unread* emails stored in by web-based email service—also leads to an arbitrary and untenable "gap" in the legal protection of electronic communications. S. Rep. No. 99-541, at 5. Under the district court's reading, the Stored Communications Act renders unlawful unauthorized access of *unopened* messages stored by web-based email services, whereas unauthorized access of *opened and saved* messages stored by such services would not violate the Stored Communications Act. *See Hately*, 309 F. Supp. 3d at 410.

But the messages a user of a web-based email service chooses *not* to delete—the messages the district court's construction of Subsection (B) leaves unprotected—are likely precisely the types of messages Congress sought to protect. By choosing to save such messages after reading them, the user indicates that the messages have sufficient personal, commercial, or other significance that they want to be able to access them again in the future. It defies logic that the unopened junk and spam email messages that a user leaves in his or her inbox or designated folder without opening would be entitled to *more* protection than those messages the user chooses to open *and* retain. We do not believe Congress intended such an absurd result when it enacted a statute intended to fill in the gaps in the then-existing privacy protections for electronic communications and therefore spur adoption of new communication technologies, like email.

IV.

In sum, the district court improperly granted Watts's motion to dismiss for failure to plausibly allege "injury to person or property" under the Virginia Computer Crimes Act. Additionally, the district court erroneously granted Watts's motion for summary judgment by concluding that previously opened and delivered emails stored in a web-based email client were not "electronic storage" for purposes of the Stored Communications Act.[10] Accordingly, we reverse the district court's dismissals of

[10] Watts also argues that the district court properly awarded him summary judgment on the Stored Communications Act claim because he did not "*intentionally* access [Hately's] email without authorization or *intentionally* exceed his authorization to access [Hately's] email." Appellee's Br. at 51. The district court did not address whether (Continued)

Hately's Virginia Computer Crimes Act and Stored Communications Act claims and remand the case to the district court for further proceedings consistent with this opinion.

REVERSED AND REMANDED

Hately's evidence was sufficient to create a dispute of fact as to intent, and therefore we decline to address that question in the first instance.