THE YALE LAW JOURNAL

REBECCA STEELE

Equalizing Access to Evidence: Criminal Defendants and the Stored Communications Act

ABSTRACT. The Stored Communications Act (SCA) poses an increasing threat to criminal defendants' constitutional rights. This Note offers the first comprehensive survey of existing appellate and federal court case law involving criminal defendants seeking access to evidence covered by the SCA. Using those findings, the Note analyzes statutory interpretations of the SCA that could allow criminal defendants to access the content of electronic communications. In cases where no such avenues are available to access exculpatory evidence, this Note concludes that the SCA's restrictions on disclosure of the content of electronic communications violate criminal defendants' constitutional rights under the Due Process Clause and the Sixth Amendment.

AUTHOR. Yale Law School, J.D. 2021; University of King's College/Dalhousie University, B.A. 2017. Thank you to Professor Tracey L. Meares for providing invaluable feedback on this project; to Professor Rebecca Wexler and Jerome D. Greco for sharing their incredibly helpful insights on this topic; and to Kate Hamilton, Joseph B. Linfield, Rachel V. Sommers, and all of the *Yale Law Journal* editors who worked on this piece for their thoughtful edits and comments. Finally, I thank Josh Feldman and my friends and family for their advice and support. Any errors are my own.

NOTE CONTENTS

INTRODUCTION 1586

I. INEQUITIES IN CRIMINAL DEFENDANTS' ACCESS TO EVIDENCE 1587

II. THE CURRENT FRAMEWORK OF THE SCA 1595
- A. The Need for Regulation 1596
- B. The End Result: The Stored Communications Act 1598

III. PATHWAYS FOR DEFENDANTS TO ACCESS INFORMATION UNDER THE SCA 1600
- A. Circumventing Subpoenas to Covered Service Providers 1601
  1. Subpoenas to Senders or Recipients 1601
  2. Cooperation with Law Enforcement to Issue Warrants 1604
  3. Interrogating Online Platforms' Classification as ECS or RCS Providers Under the SCA 1606
- B. Statutory Litigation Strategies: Exceptions to the SCA 1611
  1. Exception for Addressee or Intended Recipient 1611
  2. Exception Based on Consent 1613
  3. Outcome of Exceptions: Permissive Versus Mandatory Disclosure 1615

IV. CONSTITUTIONAL CHALLENGES TO THE SCA 1617
- A. Due-Process Rights 1619
  1. *Brady* and Prosecutorial Misconduct 1619
  2. *Wardius* and Reciprocity Requirements 1623
  3. Actual Innocence 1627
- B. Sixth Amendment Rights 1632
  1. Right to Confrontation and Cross-Examination 1633
  2. Right to Compulsory Process 1634
  3. Right to Effective Assistance of Counsel 1637

CONCLUSION 1639

INTRODUCTION

In 2016, California resident Lance Touchstone drove to San Diego to visit his sister, Rebecca Touchstone.[1] Rebecca lived with her boyfriend, Jeffrey Renteria. During the visit, Lance watched his sister's boyfriend engage in increasingly strange behavior, which culminated in Jeffrey taking Rebecca's personal firearms and threatening to harm both Lance and Rebecca. When Jeffrey finally burst into Rebecca's house and lunged towards them, Lance shot him, inflicting nonfatal wounds. Lance immediately set aside his weapon and called 911.[2]

Lance was charged with attempted murder and faced a maximum of twenty-two years in state prison.[3] He ultimately pled not guilty due to self-defense.[4] To support his case, he attempted to obtain Facebook posts from Jeffrey's account that included threats against his sister's life.[5] But the Stored Communications Act's (SCA) bar on the disclosure of the contents of electronic communications prevented Lance from accessing this potentially crucial evidence.[6] While the SCA has an exception that allows law enforcement to access the contents of electronic communications, there is no equivalent exception for criminal defendants.[7] In cases like Lance's, where law enforcement refuses to obtain information covered by the SCA, criminal defendants may have no way of accessing potentially exculpatory evidence.

Lance Touchstone is one of many criminal defendants impacted by privacy statutes that foreclose pathways for the defense to access information, while preserving such pathways for law enforcement.[8] Focusing on the SCA, this Note outlines strategies for overcoming this inequity by either working around the statute's prohibitions or working within its exceptions. In instances where neither route allows defendants to access exculpatory evidence, this Note argues that the SCA is unconstitutional as applied.

---

1. Real Party in Interest Touchstone's Opening Brief on the Merits at 9, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203).
2. *Id.*
3. *Touchstone*, 471 P.3d at 388 n.1.
4. *See id.* at 387.
5. Real Party in Interest Touchstone's Opening Brief on the Merits, *supra* note 1, at 9-11.
6. 18 U.S.C. §§ 2701-2712 (2018).
7. *Id.* § 2703.
8. *See, e.g.*, United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015); United States v. Wenk, 319 F. Supp. 3d 828 (E.D. Va. 2017); United States v. Amawi, 552 F. Supp. 2d 679 (N.D. Ohio 2008); Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019); State v. Bray, 422 P.3d 250, 256 (Or. 2018); State v. Johnson, 538 S.W.3d 32 (Tenn. Crim. App. 2017).

Part I of this Note outlines the importance of digital evidence and the structural challenges criminal defendants face in accessing it, including the "privacy asymmetries" studied by Rebecca Wexler.[9] Part II focuses on the SCA as an example of a privacy asymmetry, given the differential access to covered content afforded to the prosecution compared to the defense, and provides an overview of the statute. Working within the current SCA regime, Part III offers litigation strategies that could allow defendants to overcome barriers to accessing crucial evidence, while explaining why they may not be available or effective in many cases. Section III.A outlines pathways to evidence criminal defendants could consider to steer clear of the SCA altogether: subpoenaing senders or recipients directly, cooperating with law enforcement to secure a warrant, or challenging the classification of the online platform at issue as a provider of electronic communication services (ECS) or remote computing services (RCS) as defined by the statute. Turning to cases where the evidence in question falls within the SCA's coverage, Section III.B lays out the statutory exceptions criminal defendants can use to their advantage, including the exception for addressees or intended recipients and the exception for consent.

Finally, focusing on cases where such strategies within the current regime are not available, Part IV outlines how criminal defendants' rights under the Due Process Clause and Sixth Amendment render the asymmetrical provisions of the SCA unconstitutional. Section IV.A outlines the application of due-process jurisprudence to a criminal defendant's right to access content covered by the SCA, with a focus on arguments rooted in *Brady*[10] and prosecutorial misconduct, *Wardius*[11] and reciprocity requirements, and actual-innocence case law. Section IV.B discusses arguments grounded in the Sixth Amendment, including how a criminal defendant's rights to confrontation and cross-examination, compulsory process, and effective assistance of counsel could be violated by the denial of content covered by the SCA.

I. INEQUITIES IN CRIMINAL DEFENDANTS' ACCESS TO EVIDENCE

Digital evidence has become increasingly important in modern criminal cases. It is commonly understood as "information and data . . . that is stored on,

9. Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212 (2021).

10. Brady v. Maryland, 373 U.S. 83 (1963).

11. Wardius v. Oregon, 412 U.S. 470 (1973).

received, or transmitted by an electronic device."[12] In some cases, digital evidence comes from technologies owned and operated by law enforcement, such as gunshot-detection data,[13] location data from cell-site simulators (also known as Stingrays),[14] or facial-recognition software.[15] In other cases, digital evidence arises from devices in the possession of a victim or criminal defendant—including biometric data on a pacemaker[16] or smartwatch,[17] data collected from GPS signals,[18] and recordings from smart-home devices.[19] This Note focuses on a subset of digital evidence arising from devices in the possession of a victim, criminal defendant, or witness: the content of electronic communications like email or social media.[20]

---

12. Nat'l Inst. of Just., *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, U.S. DEP'T JUST., at ix (Apr. 2008), https://www.ojp.gov/pdffiles1/nij/219941.pdf [https://perma.cc/PHP3-CB3N].

13. *Reduce Gun Crime with Proven Gunshot Detection Technology*, SHOTSPOTTER, https://www.shotspotter.com/law-enforcement/gunshot-detection [https://perma.cc/74UX-2RZW]; *see also* Jay Stanley, *Four Problems with the ShotSpotter Gunshot Detection System*, ACLU (Aug. 24, 2021), https://www.aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system [https://perma.cc/6KDQ-LEBC] (describing civil-liberties problems with gunshot-detection technology, including increased policing of communities of color).

14. *Street-Level Surveillance: Cell-Site Simulators/IMSI Catchers*, ELEC. FRONTIER FOUND. (Aug. 28, 2017), https://www.eff.org/pages/cell-site-simulatorsimsi-catchers [https://perma.cc/9USV-BE7C].

15. *Accelerate Your Investigative Leads*, CLEARVIEW AI, https://www.clearview.ai/law-enforcement [https://perma.cc/3WTH-MH3X]; *see also* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/2KQM-8UXG] (describing problems with facial-recognition technology, including accuracy issues and potential violations of due process).

16. Cleve R. Wootson Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story*, WASH. POST (Feb. 8, 2017), https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story [https://perma.cc/4UE3-6QYJ].

17. Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y. TIMES (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html [https://perma.cc/4TLT-DNBT].

18. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/8GNK-JSMP].

19. Ángel Díaz, *Law Enforcement Access to Smart Devices*, BRENNAN CTR. FOR JUST. (Dec. 21, 2020), https://www.brennancenter.org/our-work/research-reports/law-enforcement-access-smart-devices [https://perma.cc/6UHY-ZU4B].

20. Joseph Goldstein, *In Social Media Postings, a Trove for Investigators*, N.Y. TIMES (Mar. 2, 2011), https://www.nytimes.com/2011/03/03/nyregion/03facebook.html [https://perma.cc/6QS3-HZPZ].

Digital evidence first became prominent in cases involving electronic crime or cybercrime, such as prosecutions for credit-card fraud or images depicting child sexual abuse.[21] For these types of crimes, evidence was necessarily digital. However, the increasing prevalence of technology and social media has led to the use of digital evidence in criminal cases more broadly: even if the conduct at issue took place offline, there may be online records central to the prosecution or defense's case. For example, location records that can be derived from a criminal defendant's cell phone may be crucial to establish an alibi[22]—or may support the prosecution's theory that the defendant was present at the scene of the crime.[23] A criminal defendant's online communications could bolster a claim of self-defense[24]—or show interactions that establish a criminal conspiracy.[25] As we increasingly rely on smartphones, personal computers, programmable home appliances, and other digital devices, digital evidence will continue to become more important in criminal cases.[26]

In addition to its growing availability and relevance, digital evidence has also become more prominent because of its unparalleled level of detail and specificity. Social-media evidence serves as a telling example. Attorneys Justin P. Murphy and Adrian Fontecilla contrast social-media evidence with the information that can be derived from phone records:

> When a phone company responds to a government subpoena or search warrant, it may provide call or message logs. In contrast, when a social media company like Facebook responds to a government subpoena, it

---

21. *Digital Evidence and Forensics*, NAT'L INST. JUST., https://nij.ojp.gov/digital-evidence-and-forensics [https://perma.cc/Q3FR-UMQN].

22. *See* Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone.*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html [https://perma.cc/G3ME-YMVU].

23. *See, e.g.*, United States v. Meza, 800 F. App'x 463, 466-67 (9th Cir. 2020) (Korman, J., concurring) ("GPS data puts [the defendant] at the scene of the crime when it occurred . . . .").

24. Facebook, Inc. v. Pepe, 241 A.3d 248, 251-52 (D.C. 2020).

25. State v. Davis, 310 Neb. 865, 877 (2022) (considering social-media evidence to affirm the defendant's conviction of conspiracy to commit robbery, including the fact that "Davis used social media messages with Cooke to ensure the scheme went according to plan" and that "[i]n social media messages to Cooke, Davis expressed interest in keeping particular items that they had taken").

26. *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 488 (2013) ("It is no secret that the nature of criminal evidence is changing. Information is less and less likely to be found in physical forms (like a day planner or printed photographs found in the home) than in more abstract places where the strictures of the Constitution play a less defined role (like the bits and bytes of an iPhone, Flickr account, or Gmail calendar server).").

> could provide the user's profile, wall posts, photos that the user uploaded, photos in which the user was tagged, a comprehensive list of the user's friends with their Facebook IDs, and a long table of login and IP data.[27]

Additionally, as social-media companies have moved toward offering location-based services, they are also able to offer precise location information.[28]

Given the wealth of information that can be gleaned from user accounts, it should come as no surprise that law-enforcement requests for information directed at online platforms have grown significantly over the past decade. Data published in social-media companies' transparency reports demonstrate that the number of requests for user information that Facebook, Google, and Twitter have received from the U.S. government has more than quadrupled over the past seven years—from under 50,000 total requests in 2013 to 226,301 requests in 2020.[29] These companies do not publicly release breakdowns categorizing specific types of requests; therefore, it is impossible to capture the precise number of requests issued specifically pursuant to criminal proceedings. However, Facebook notes that "[t]he vast majority of [government] requests relate to criminal

---

27. Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 1, 4 (2013) (citing Carly Carioli, *When the Cops Subpoena Your Facebook Information, Here's What Facebook Sends the Cops*, PHOENIX (Apr. 6, 2012, 8:30 AM), https://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx [https://perma.cc/555D-X8QU]).

28. *Id.* at 3.

29. In 2013, Facebook received 23,598 requests for user data from the U.S. government, Twitter received 1,735 of such requests, and Google received 21,492 of such requests, totaling 46,825 government requests for user data between all three Internet Service Providers (ISPs). In 2020, Facebook received 122,790 requests for user data from the U.S. government, Twitter received 6,672 of such requests, and Google received 96,839 of such requests, totaling 226,301 government requests for user data between all three companies. *See Transparency Center: Government Requests for User Data*, META, https://transparency.fb.com/data/government-data-requests [https://perma.cc/2X3E-VX4M] (click "Download (CSV)"); *Transparency: Information Requests*, TWITTER, https://transparency.twitter.com/en/reports/information-requests.html#2020-jan-jun [https://perma.cc/QS7H-MPWZ]; *Transparency Report: Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview [https://perma.cc/63L6-V2GS]. These three providers were selected because they are the only companies involved in multiple cases considered in this study where criminal defendants sought access to content in a way that implicated the Stored Communications Act (SCA).

cases,"[30] while Google similarly confirms that "most [government] requests are issued in the context of criminal investigations."[31]

The success rates of these requests are relatively high. In 2019, Facebook produced user data in 88% of cases,[32] Google produced data in 80.5% of cases,[33] and Twitter produced data in 66% of cases.[34] This data points towards a growing use of social-media evidence in criminal prosecutions.

However, there has not been a comparable increase in access to social-media evidence on the part of criminal defendants. Of the three companies listed above, Twitter is the only company that publicizes data on requests for information from nongovernment entities.[35] The number of requests for information that Twitter receives from nongovernmental entities, which includes criminal defendants as well as civil litigants,[36] is strikingly lower than the number of requests the company receives from government entities. In 2020, for example, Twitter received 6,672 information requests from the U.S. government, and 137 nongovernment information requests from individuals or entities in the United States.[37] While these numbers are imprecise insofar as they speak to government and nongovernment requests generally as opposed to prosecution and defense requests specifically, these statistics nonetheless shed light on overall trends that are applicable to information requests in criminal proceedings.

Furthermore, there is also a significant discrepancy between the success rates of requests from governmental and nongovernmental actors. Compared to the 59.5% of U.S. government requests for which Twitter produced information in

30. *Further Asked Questions: What Is a Government Data Request?*, FACEBOOK, https://transparency.fb.com/data/government-data-requests/further-asked-questions [https://perma.cc/7KHM-3DQL].

31. *Requests for User Information FAQs: What Is a Government Request for User Information?*, GOOGLE, https://support.google.com/transparencyreport/answer/9713961#zippy=%2Cwhat-is-a-government-request-for-user-information [https://perma.cc/PP57-97P6]. Twitter does not provide information on the breakdown of government requests.

32. META, *supra* note 29.

33. GOOGLE, *supra* note 29.

34. TWITTER, *supra* note 29.

35. *Id.*

36. "Twitter receives requests for account information from non-governmental parties around the world. These typically include civil actions, such as a divorce proceeding, as well as requests made by criminal defendants, where they are typically seeking account information in support of their legal defense." *Id.*

37. *Twitter Transparency Information Request Tables July-December*, TWITTER (2020), https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec [https://perma.cc/27FV-B8LB]. For access to Twitter's transparency report, click "Download Report," then click "Download CSV," and combine the data from the July-December and January-June tables.

2020, Twitter produced information in response to only 10% of nongovernmental information requests within the United States.[38] While there have been minor fluctuations in success rates, the chasm between Twitter's response to governmental and nongovernmental actors has persisted.[39]

There are several explanations both for the lower number of requests made by nongovernment actors and their lower success rates. This Note focuses on the explanations that apply to criminal defendants compared to law enforcement. First, online platforms have developed infrastructures that make it much easier for law enforcement to request user information. For example, Facebook,[40] Google,[41] and Twitter[42] all have portals that give law enforcement a specific pathway to request information from user accounts. There is no equivalent pathway for criminal defendants.

Second, pursuing and utilizing digital evidence from online platforms can be a technical and resource-intensive process, which is exacerbated by the fact that criminal defendants and their counsel cannot access this information through a streamlined portal in the way law enforcement can. In addition, across the country, there are only two public-defense offices that have digital-forensics labs.[43] The Legal Aid Society of New York's lab in Manhattan is by far the most developed. Indeed, its equipment cost $100,000.[44] But by comparison, the equipment in the Manhattan District Attorney's office's lab cost $10 million, giving them significantly increased capacity to discover and investigate digital evidence.[45] In

38. *Id.*

39. Between 2015 and 2020, Twitter's compliance rates for government-information requests ranged from a low of 59% compliance to a high of 82% compliance. *Id.* Twitter had significantly diminished compliance rates for nongovernment information requests during the same period: a low of 6% compliance to a high of 24% compliance. *Id.*

40. *Law Enforcement Online Requests*, FACEBOOK, https://www.facebook.com/records/login [https://perma.cc/2B53-9XM5].

41. *Law Enforcement Request System*, GOOGLE, https://lers.google.com/signup_v2/landing [https://perma.cc/G8HF-558H].

42. *Law Enforcement Request*, TWITTER, https://help.twitter.com/forms/lawenforcement [https://perma.cc/QPG5-WAH6].

43. The *New York Times* conducted a review of public-defense offices and found that at the time of publication, only the Legal Aid Society of New York had a digital-forensics lab, while the public defender's office in Philadelphia was in the process of establishing one. A few other offices have some limited digital-forensics capacity in the form of a single extraction device or an in-house expert. *See* Hill, *supra* note 22. With sufficient resources, public-defense digital-forensics labs can investigate "emails, text messages, call logs, location history, photos, metadata and more – even material that has been deleted," and moreover, can "capture[] it in a format that can hold up in court, as opposed to evidence that could have been tampered with or forged." *Id.*

44. *Id.*

45. *Id.*

cases where a criminal defendant subpoenas information from an online platform and the company moves to quash based on the SCA, frequently underresourced criminal defense attorneys will be up against the high-powered legal teams of companies like Facebook, Google, and Twitter.

Finally, and perhaps most importantly, criminal defendants may have no established legal avenues to seek out social-media information due to what Rebecca Wexler has termed "privacy asymmetries."[46] Privacy asymmetries are "privacy statutes that permit courts to order disclosures of sensitive information if requested by law enforcement, but not if requested by the defense."[47] Wexler highlights how political actors and academics alike have centered their privacy-protection debates around finding a balance between individual privacy interests and law-enforcement needs.[48] By contrast, criminal defendants' interests are consistently left out of such debates, resulting in statutes that create an exception to a general bar on the disclosure of information for law enforcement, but no equivalent exception for criminal defendants.[49] In some cases, this imbalance is created when a statute indicates information it covers can be obtained through a search warrant—an investigative tool available exclusively to the state—but makes no mention of other forms of judicial process available to the defense, including subpoenas.[50] In other cases, the statute bars access to specified information but explicitly delineates an exception allowing disclosure to a law-enforcement agency or government entity, without accounting for other actors' need to access such information.[51] In both scenarios, these asymmetrical statutes specifically account for a pathway law enforcement can use to access private information without addressing how criminal defendants can accomplish the same ends. Wexler suggests that this imbalance is a result of legislative oversight, not reasoned deliberation.[52]

These privacy asymmetries are not entirely unique to digital evidence, although it is worth noting that privacy statutes are disproportionately crafted in response to technological advances.[53] Given the increasing availability of data in

---

46. Wexler, *supra* note 9, at 215.

47. *Id.*

48. *Id.* at 218.

49. *Id.* at 219, 229-30.

50. *See, e.g.*, *id.* at 265 (citing 39 U.S.C. § 404(c) (2018)).

51. *See, e.g.*, *id.* at 269 (citing 18 U.S.C. §§ 2702(b)(7), 2703 (2018)); *id.* at 271 (citing 18 U.S.C. § 2710(b)(2)(C) (2018)); *id.* at 275 (citing 26 U.S.C. § 6103(i)(1)(A) (2018)).

52. *Id.* at 242-46.

53. *See* Murphy, *supra* note 26, at 499-500 (identifying the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, and the Right to Financial Privacy Act of 1978, among others, as examples of privacy statutes motivated at least in part by technological progress).

the digital economy, the effects of privacy asymmetries are becoming more pronounced.[54] For example, if a witness's Facebook messages might contain *inculpatory* evidence, law-enforcement agents have an incentive to seek them out and can use one of the law-enforcement exceptions built into privacy statutes to do so. But if a witness's Facebook messages contain *exculpatory* evidence, the same agents have no incentive or obligation to employ the law-enforcement exception to access the information. Some law-enforcement actors have even argued that the law-enforcement exception would not allow them to do so.[55] Given that this type of digital evidence is in the possession of third parties as opposed to the government, the prosecution's discovery-disclosure obligations under *Brady* and applicable statutes will generally not apply.[56] This could leave the exculpatory evidence entirely outside the reach of criminal defendants.

As scholars have established, asymmetries in access to evidence carry troubling policy implications. Most notably, privacy asymmetries risk the accuracy and fairness of criminal proceedings. As Wexler describes,

> In the U.S. adversarial criminal legal system, defense counsel are the sole actors tasked with investigating evidence of innocence. Law enforcement has no constitutional, statutory, or formal ethical duty to seek out evidence of innocence. Therefore, statutes that selectively suppress defense investigations selectively suppress evidence of innocence.[57]

Ion Meyn similarly points to information disparities as "inconsistent with the design of the adversarial system" and argues that they result "in a factual deficit that undermines the legitimacy of outcomes," creating a situation where "[a] criminal defendant must sip from the cup of his opponent."[58] This outcome is particularly concerning given the disparate impact of these asymmetrical policies on marginalized communities. Indeed, due to pervasive disparities in policing, charging, and sentencing within the criminal justice system, the impacts of

---

54. *See* Wexler, *supra* note 9, at 216-18.

55. *See, e.g.*, State v. Bray, 422 P.3d 250, 257 (Or. 2018) (remarking that the district attorney took the position that he could not seek a search warrant without probable cause that it would lead specifically to evidence of a crime, as opposed to evidence of innocence).

56. *See infra* Section IV.A.1.

57. Wexler, *supra* note 9, at 212.

58. Ion Meyn, *Discovery and Darkness: The Information Deficit in Criminal Disputes*, 79 BROOK. L. REV. 1091, 1093, 1126 (2014).

these asymmetries are felt disproportionately by Black communities[59] and other communities of color,[60] as well as communities impacted by poverty.[61]

Beyond the widely discussed implications of this imbalance on justice, fairness, and accuracy within the criminal justice system, these asymmetrical statutes also raise constitutional concerns.[62] The imbalance itself calls into question the Supreme Court's jurisprudence mandating a particular balance of forces between the accused and his accuser.[63] But even putting this asymmetry aside, the bars on criminal defendants' access to information implicate defendants' standalone rights to due process and a fair trial. These standalone rights arguably require that defendants be allowed access to exculpatory private information independent from the question of whether the prosecution can access such evidence. Denying criminal defendants access to digital evidence while granting that access to prosecutors creates two distinct but overlapping issues — one related to a standalone right of access, the other related to asymmetry. In light of the growing importance of social-media evidence in criminal cases, it is crucial to explore pathways that could allow criminal defendants to access the contents of electronic communications and to consider the constitutional implications when they cannot.

II. THE CURRENT FRAMEWORK OF THE SCA

To analyze the barriers criminal defendants face to accessing information covered by the SCA, it is important to understand the history of the statute and its parameters as it applies today. This Part lays out the history of the statute and offers a brief summary of its coverage: first, by outlining the incongruity between privacy jurisprudence and emerging technology that led to the creation of the SCA, and second, by describing the coverage of the statute itself.

---

59. *See, e.g.*, Elizabeth Hinton, LeShae Henderson & Cindy Reed, *An Unjust Burden: The Disparate Treatment of Black Americans in the Criminal Justice System*, VERA INST. JUST. (May 2018), https://www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf [https://perma.cc/6UWB-D8UJ].

60. *See, e.g.*, Ashley Nellis, *The Color of Justice: Racial and Ethnic Disparity in State Prisons*, SENT'G PROJECT (Oct. 2021), https://www.sentencingproject.org/wp-content/uploads/2016/06/The-Color-of-Justice-Racial-and-Ethnic-Disparity-in-State-Prisons.pdf [https://perma.cc/KE2K-LFXY].

61. *See, e.g.*, Paul D. Butler, *Poor People Lose:* Gideon *and the Critique of Rights*, 122 YALE L.J. 2176 (2013).

62. For an in-depth discussion of the constitutional concerns posed by the SCA, see *infra* Part IV.

63. *See, e.g.*, Wardius v. Oregon, 412 U.S. 470, 474-79 (1973).

A. The Need for Regulation

Shortly after the advent of digital evidence came the realization that traditional privacy jurisprudence was ill-equipped to regulate it. Fourth Amendment law developed in the context of traditional physical evidence and eyewitness testimony.[64] Although "the Fourth Amendment protects people, not places,"[65] the nature of evidence at issue in foundational Fourth Amendment case law has inevitably resulted in jurisprudence that protects physical things. Therefore, the Fourth Amendment's protections of "people" are deeply tied to the physicality of those people, including, for example, what police officers see or hear them do,[66] the physical boundaries of their homes,[67] and what is in physical reach of their person.[68] Evidence that exists solely online can be challenging to categorize within the norms of traditional Fourth Amendment case law.

In addition to the subject matter of existing Fourth Amendment case law making it difficult to analogize to electronic evidence, the tests developed to establish the scope of Fourth Amendment protection are ill-equipped to extend protection to evidence that arises in the modern internet era. To determine which forms of evidence are protected by the Fourth Amendment and which are not, the Supreme Court established a test that hinges on individuals' "reasonable expectation[s] of privacy."[69] An individual's justifiable reliance on a reasonable expectation of privacy triggers constitutional protection. Yet, with the advent of the third-party doctrine, the Supreme Court definitively held that individuals have no reasonable expectation of privacy in information that they convey to other people.[70] Specifically, the third-party doctrine mandates that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[71]

---

64. Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005) (recommending new procedural doctrines tailored to digital evidence in light of the fact that "[t]he law of criminal procedure has evolved to regulate the mechanisms common to the investigation of physical crimes, namely the collection of physical evidence and eyewitness testimony" and that "[t]he new ways of collecting [digital] evidence are so different that the rules developed for the old investigations often no longer make sense for the new").

65. Katz v. United States, 389 U.S. 347, 351 (1967).

66. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 30 (1968).

67. *See, e.g.*, Collins v. Virginia, 138 S. Ct. 1663, 1671 (2018).

68. *See, e.g.*, Chimel v. California, 395 U.S. 752, 768 (1969).

69. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

70. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (establishing the third-party doctrine).

71. *Id.*

Notably, all or almost all of a given person's online existence—the emails they send to coworkers and to family, the documents they have in cloud storage, the photos they text to their friends—are held by third parties. In the context of digital evidence, third parties include email providers, cloud-storage providers, social-media providers, online-banking providers, and other third-party entities. Any information that is "online" is by definition hosted on the servers of a third party, as opposed to (or in addition to) being stored locally by users themselves. Individuals might expect confidential messages sent over the internet to be considered private, but the third-party doctrine instructs that they may not be.

As Orin S. Kerr explains, attempts at third-party evidence collection became more prominent after certain technological advances because "perpetrators of physical crimes generally keep the evidence to themselves rather than give it to third parties."[72] This is no longer true in the internet era. In light of the changing ways in which modern evidence is accumulated, traditional Fourth Amendment rules do not always serve their intended purposes in the digital context.[73] Because of the poor fit between Fourth Amendment doctrine and digital evidence, users' privacy interests in digital information have increasingly been regulated by statute.[74]

The Electronic Communications Privacy Act (ECPA) of 1986[75]—which includes the SCA,[76] originally enacted as Title II of the ECPA[77]—was designed to fill this gap in privacy protections. The ECPA predates the World Wide Web.[78] The legislative history shows that the ECPA was directly responsive to concerns that the Fourth Amendment did not adequately protect privacy interests when confronted with emerging technology.[79] In the wake of the Supreme Court's development of the third-party doctrine, the Senate Committee on the Judiciary

---

72. Kerr, *supra* note 64, at 294.

73. *See id.* at 306-07.

74. *See* Murphy, *supra* note 26, at 486-88.

75. 18 U.S.C. §§ 2510-2523 (2018).

76. *Id.* §§ 2701-2712.

77. Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860.

78. Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 573 (2007).

79. *See* S. REP. NO. 99-541, at 1-2 (1986) ("When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the fourth amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such

was particularly concerned about the "legal uncertainty" surrounding digital evidence.[80] Furthermore, online platforms were increasingly collecting and storing information, and, as nongovernment actors, they were not governed by the Fourth Amendment at all.[81] However, as legislative research by scholars including Marc J. Zwillinger and Christian S. Genetski has revealed, "[g]iven the focus on the Fourth Amendment, Congress appears simply to have overlooked the potential concerns of non-state actors seeking compulsory access to information held by ISPs [Internet Service Providers]."[82] The statute, drafted against the particular backdrop of the shortcomings of the Fourth Amendment, was enacted before the emergence of most modern forms of electronic communications. It is therefore unsurprising that the statute is ill-equipped to account for the needs of nongovernment actors seeking access to communications transmitted over cutting-edge technologies.

B. The End Result: The Stored Communications Act

The provisions of the ECPA that deal with access to stored electronic communications are referred to as the Stored Communications Act.[83] The SCA applies to two different types of providers: ECS providers and RCS providers. The statute defines ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[84] The legislative history offers telephone companies and electronic mail companies as examples.[85] RCS refers to "the provision to the public of computer storage or processing services by means of an electronic communications system."[86] The legislative history notes that "businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing."[87] These categories were based on

intrusions."). At the time, the Senate Committee on the Judiciary offered the telephone as an example. *Id.* at 2. Now, their conclusion clearly applies to a much wider array of technologies and forms of communication.

80. *Id.* at 5; *see also id.* at 3 ("For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.").

81. Zwillinger & Genetski, *supra* note 78, at 575-76.

82. *Id.* at 577.

83. 18 U.S.C. §§ 2701-2712 (2018).

84. *Id.* § 2510(15).

85. S. REP. No. 99-541, at 14.

86. 18 U.S.C. § 2711(2) (2018).

87. S. REP. No. 99-541, at 10.

a 1980s understanding of electronic communications, before many of the forms of electronic communication central to today's evidence disputes even existed.

Using these arguably outdated categories of statutory coverage, courts have attempted to determine whether and how modern providers fall under the statute. Cellphone service providers like Sprint[88] and email service providers like AOL,[89] Microsoft, and Google[90] have been found to be ECS providers. Social-media companies like Facebook and MySpace have also been categorized as ECS providers because they "provide private messaging or email services."[91] These initial categorizations of modern online platforms have largely gone unquestioned, but they arguably deserve further attention.[92]

Section 2702 of the SCA is the provision of the statute relevant to criminal defendants attempting to access electronic communications. It applies to providers who make their services available "to the public" at large, whether with or without a fee.[93] Subsection (a) speaks to prohibitions. Generally speaking, this provision bans ECS and RCS providers from disclosing the content of communications and from disclosing noncontent records to government entities.[94] However, subsection (b) outlines a number of exceptions where providers *may* "divulge the contents of a communication," including "to an addressee or intended recipient" of the communication, and "with the lawful consent of the originator or an addressee or intended recipient" of the communication.[95] This

---

88. *See* Jayne v. Sprint PCS, No. CIV S-07-2522, 2009 WL 426117, at *6 (E.D. Cal. Feb. 20, 2009); *see also In re* Application of the U.S. for an Ord. for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) (holding that cellphone-service providers "clearly fit within [the] definition" of electronic communication services (ECS) providers in the SCA).

89. *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008).

90. Hately v. Watts, 917 F.3d 770, 790 (4th Cir. 2019) ("[W]e 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.").

91. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010).

92. See *infra* Section III.A.3 for an argument that, because of their business model, modern social-media companies generally do not constitute ECS providers or remote computing service (RCS) providers, as defined by the statute.

93. 18 U.S.C. § 2702(a)(1) (2018). Orin S. Kerr explains that "providers do not provide services to the public if its ECS or RCS services are available only to users with special relationships with the provider. If a university provides accounts to its faculty and students or a company provides corporate accounts to its employees, those services are not available to the public." 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, 1226 (2004). This means that individuals using the services of nonpublic providers, including those who use email accounts provided by their school or place of work, are subject to fewer protections. *See id.* at 1226-27.

94. *See* 18 U.S.C. § 2702(a) (2018).

95. *Id.* § 2702(b)(1), (3).

provision also outlines specific channels to enable government entities to access the contents of the communication,[96] and includes a cross-reference to other components of the statute, including § 2703, which provides additional mechanisms for government entities to access electronic communications.[97]

III. PATHWAYS FOR DEFENDANTS TO ACCESS INFORMATION UNDER THE SCA

To understand the impact of privacy asymmetries like those in the SCA on criminal defendants' access to evidence, it is important to consider how these statutory provisions function in practice. In this Part, I explore strategies criminal defendants and their counsel can use to access evidence in a way that is consistent with the provisions of the SCA. First, I outline a number of paths criminal defendants could pursue to access the contents of electronic communications by circumventing subpoenas to covered service providers altogether. Given that the SCA restricts subpoenas to covered ECS and RCS providers, this can be achieved by (1) avoiding covered ECS and RCS providers by subpoenaing senders or recipients of the communications directly; (2) avoiding subpoenas by enlisting the assistance of law enforcement to issue warrants; and (3) arguing that the company in question does not constitute an ECS or RCS provider as covered by the SCA. Second, for cases where it is not possible to avoid the reach of the SCA, I offer strategies for working within its exceptions. Defendants might be able to work within either the exception allowing addressees or intended recipients to access the contents of electronic communications, or the exception allowing ECS and RCS providers to disclose the contents of communications upon consent. I also consider whether disclosure under these exceptions is mandatory or permissive, arguing in favor of the former.

While these avenues could prove fruitful for some defendants and are worth pursuing when available, this Note shows that they will frequently be insufficient to allow for meaningful access to evidence. To provide an accurate assessment of the state of the law and how various courts have interpreted defendants' claims to evidence covered by the SCA, this Part uses the first comprehensive survey of appellate and federal court cases involving criminal defendants seeking access to content covered by the SCA.[98]

---

96. *Id.* § 2702(b)(6)-(9).

97. *See id.* § 2703.

98. To identify these cases, I reviewed all of the cases on LexisNexis citing 18 U.S.C. § 2702 (2018) as of November 2021. Seventeen of these cases involved criminal defendants seeking evidence.

A. Circumventing Subpoenas to Covered Service Providers

When judges decline to allow or enforce defense subpoenas to covered providers under the SCA, they often simultaneously recommend that defendants pursue alternative means of accessing evidence. Online platforms have invoked the same arguments in their motions to quash subpoenas. The most common proposed paths forward are subpoenaing senders or recipients directly[99] and working with law enforcement to issue a warrant instead of a subpoena.[100] Some litigants have also suggested that the business model of social-media companies like Facebook distinguishes them from the ECS and RCS providers that fall within the SCA's coverage, and therefore that subpoenas served on Facebook and companies with the same business model fall outside of the statute's ambit.[101]

In this Section, I explore the limited scenarios where it may be possible for defendants to access the content of online communications by circumventing the SCA entirely. In doing so, this Section also highlights why these three options might not provide meaningful access to evidence.

1. Subpoenas to Senders or Recipients

As discussed above, the SCA does not apply to individuals disclosing electronic communications that they have sent or received themselves. Instead, it applies specifically to ECS and RCS providers. For that reason, judges and online

Given that this list included appeals involving the same criminal defendant, the list constituted fourteen discrete cases. I supplemented this search with general keyword searches (revealing one additional case that mentioned the SCA only in a footnote) and cross-referenced the list I came up with against cases cited in existing academic literature on the SCA. That search revealed one additional state-court case that is not available online. *See* Colone v. Superior Ct. (*GitHub*), No. S265307 (Cal. Jan. 13, 2021) (judgment and order denying petition for review); *see also In re* Application of: Joseph Colone, No. CFP-20-517083 (Cal. Sup. Ct. July 28, 2020) (order denying motion to compel production of records); Colone v. Superior Ct., No. CPF20517083 (Cal. Ct. App. Oct. 21, 2020) (denying petition for mandate or other relief). However, it is important to note that many trial-level state-court orders and decisions are not available on search engines like LexisNexis and Westlaw and are therefore not included in this survey. Subpoenaed providers themselves may be the only actors who are able to identify the full list of cases across all jurisdictions implicating the SCA in criminal defendants' attempts to access evidence. *See* Petition for a Writ of Certiorari, Appendix F, Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 741 (Cal. 2018), *cert. denied*, 140 S. Ct. 2761 (2020) (listing numerous cases not available on LexisNexis or Westlaw).

99. *See, e.g.*, R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734, at *6 (Mass. Dec. 15, 2020); United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015); State v. Johnson, 538 S.W.3d 32, 70 (Tenn. Crim. App. 2017).

100. *See, e.g.*, Facebook, Inc. v. Pepe, 241 A.3d 248, 252-53 (D.C. 2020).

101. San Diego County District Attorney Intervenor Brief at 4-5, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203).

platforms have frequently proposed subpoenaing senders or recipients as a workaround to the SCA in scenarios where criminal defendants unsuccessfully subpoenaed a covered ECS or RCS provider.[102] In some scenarios, this strategy could be successful. However, there are numerous situations where subpoenas directed at the senders or recipients of electronic communications will not be a feasible solution.

First, there are certain scenarios in which obtaining information directly from senders or recipients will prove impossible. The most obvious example occurs when the account holders are no longer alive. Criminal defendants who have been charged with murder may have an interest in obtaining evidence from the social-media accounts of the murder victim. Alternatively, the account holder may have passed away due to an unrelated cause or be otherwise unreachable. The prevalence of this issue is borne out in current SCA case law. Indeed, multiple cases involve defendants seeking information from account holders who are no longer alive.[103]

Another situation in which criminal defendants may be wholly unable to access information from senders or recipients occurs when the communications the defendants seek could implicate the sender's or recipient's Fifth Amendment right against self-incrimination. In criminal cases, this issue could be significant whenever a defendant seeks content that implicates another actor as a perpetrator. For example, in *Facebook, Inc. v. Superior Court*, Lance Touchstone sought to fight his attempted murder charges by challenging a court order quashing his subpoena of Facebook for material from the alleged victim Jeffrey Renteria's account.[104] Touchstone sought to obtain information from the account that included death threats, drug usage, and illegal firearm possession — all evidence of unlawful activity.[105] As counsel for Touchstone pointed out, "Renteria has colorable Fifth Amendment rights against self-incrimination that would support a refusal to produce the records, in the unlikely event that he were to avail himself

102. *See, e.g.*, *Pierce*, 785 F.3d at 842 (describing Facebook's argument that "the appropriate method for obtaining . . . content was to subpoena a user directly" and faulting the defendant for "fail[ing] to subpoena [the witness] and the individual who created the account in his name, the two direct potential sources for the contents of the account"); *Johnson*, 538 S.W.3d at 37 (holding that "the defendants cannot obtain the contents of the electronic communications from any of the service providers" but that "nothing prevents the defendants in this case, generally, from obtaining the type of electronic communications at issue via a subpoena issued . . . to the witnesses themselves").

103. *See, e.g.*, *Hunter*, 417 P.3d 725 (evaluating a lower court's order that internet social-media providers produce communications from the murder victim's account); People v. Q.H., No. A142771, 2016 WL 5118287, at *13 (Cal. Ct. App. Sept. 21, 2016) (declining to determine if the SCA prohibited pretrial access to the victim's Instagram account).

104. *Touchstone*, 471 P.3d 383.

105. *Id.* at 388-89.

to the criminal justice process."[106] Renteria's invocation of his Fifth Amendment rights would create another scenario where a subpoena directed at an account holder could be impossible to execute.[107]

In other circumstances, subpoenas directed at senders or recipients may be possible to execute, but ultimately prove to be ineffective. Subpoenaing users directly may result in the spoilation of evidence, or alternatively, the subpoenas may be rendered ineffective because of deletions before their issuance. The Facebook records of the alleged victim in *Touchstone*, Jeffrey Renteria, again serve as an instructive example. Renteria was not originally notified of defense counsel's efforts to secure his social-media records due to the trial court's concern that "such notification may lead to tampering with or destruction of evidence."[108] However, the Court of Appeals's ruling on the applicability of the SCA to the records was publicized in local media, at which point the alleged victim deactivated his Facebook account and destroyed the previously available information.[109] It is not uncommon for the senders or recipients of relevant content to have interests contrary to those of the defendant seeking access to it. While sanctions will be applicable to individuals who refuse to comply with a subpoena, they may not apply to individuals who delete content from their accounts *before* the issuance of the subpoena. Moreover, sanctions will not necessarily result in evidence being produced to the defendant.

A final reason that subpoenas to senders or recipients may be ineffective is that these senders or recipients frequently serve as witnesses for the prosecution.[110] Serving subpoenas on these witnesses will force the defendant to reveal at least some component of their trial strategy to the prosecution prematurely, which may hinder their ability to make their case. For these reasons, defendants will not always be able to access electronic communications via subpoenas to senders or recipients.

---

106. Real Party in Interest Touchstone's Opening Brief on the Merits, *supra* note 1, at 19.

107. *See* Supplemental Brief by Real Parties Sullivan and Hunter Regarding New Authorities Pursuant to California Rule of Court 8.520(d) at 5, *Hunter*, 417 P.3d 725 (No. S230051) (explaining the impossibility of subpoenaing the relevant witness because she was represented by counsel and invoked her Fifth Amendment rights).

108. Real Party in Interest Touchstone's Opening Brief on the Merits, *supra* note 1, at 23.

109. *Id.*

110. *See, e.g.*, United States v. Pierce, 785 F.3d 832 (2d Cir. 2015); *Touchstone*, 471 P.3d 383; State v. Johnson, 538 S.W.3d 32 (Tenn. Crim. App. 2017); R.C. v. Chilcoff, No. SJ-2020-0081, 2020 WL 8079734 (Mass. Dec. 15, 2020).

2. *Cooperation with Law Enforcement to Issue Warrants*

To circumvent the subpoena process, judges and online platforms have suggested that criminal defendants barred from obtaining evidence by the SCA cooperate with law enforcement to obtain a warrant for the information they are seeking. Whereas the previous strategy relied on a subpoena but avoided directly implicating the online platforms hosting the information, this strategy involves those platforms but avoids the limitations of a subpoena. This course of action capitalizes on §§ 2702(b)(2) and 2703 of the SCA, which together allow covered providers to disclose the contents of communications to a government entity pursuant to a warrant.[111] This path is not available to criminal defendants independently, because defense counsel do not have access to warrants and public defenders' offices do not qualify as government entities under the statute.[112]

The logic of this strategy is that prosecutors have a constitutional duty to seek the truth, not a conviction.[113] However, the feasibility of cooperation between criminal defendants and prosecutors is questionable. Indeed, relying on the state to issue a warrant for information requested by the defendant is, at worst, impossible and, at best, subject to the prosecutor's discretion. While online platforms have suggested that this could be a successful path forward,[114] the legal arguments have only been explored in a small number of cases.

The California Supreme Court ordered briefing on whether a trial court could order the prosecution to issue a search warrant on behalf of the defense,[115] but ultimately decided the case in question on different grounds.[116] In two criminal cases implicating the SCA, trial courts have issued orders compelling the

---

111. 18 U.S.C. §§ 2702(b)(2), 2703 (2018).

112. United States v. Amawi, 552 F. Supp. 2d 679, 680 (N.D. Ohio 2008) (holding that "the judiciary and its components, including the Federal Public Defender" are not government entities and therefore cannot obtain a court order under the SCA).

113. *See, e.g.*, Bennett L. Gersham, *The Prosecutor's Duty to Truth*, 14 GEO. J. LEGAL ETHICS 309, 313 (2001) ("[T]he prosecutor has a legal and ethical duty to promote truth and to refrain from conduct that impedes truth.").

114. For example, counsel for Facebook and Instagram have suggested in litigation "that defense counsel might 'work[] with the prosecutor to obtain' the requested information via an additional search warrant issued by the government." Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 731 (Cal. 2018).

115. Facebook, Inc. v. Superior Ct. (*Touchstone*), 408 P.3d 406 (Cal. 2018).

116. Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 401-02 (Cal. 2020) (remanding to allow the trial court to reconsider Facebook's motion to quash the criminal defendant's underlying subpoena based on an evaluation of whether the subpoena was supported by good cause).

prosecution to obtain social-media records on behalf of the defendant.[117] Illustrating the limitations of this path, neither defendant ultimately obtained the information sought. In one case, it is not clear why.[118] In the other, the state sent the online platform an unsuccessful subpoena for the records.[119] But when the district attorney refused to send a search warrant, the court determined that it would not require the state to obtain one.[120] The district attorney argued that "to apply for a search warrant, he would have to aver that he had probable cause to believe that a search would produce 'evidence of a crime.'"[121] The trial court disagreed with the prosecution's analysis on the necessity of evidence of a crime, but ultimately held that it could not force the district attorney to pursue the warrant.[122] Applicable Oregon law, comparable to the requirements in *Brady v. Maryland*,[123] requires prosecutors to turn over materials in their "possession or control,"[124] and the court held that evidence in the possession of third parties like online platforms did not fall into that category.[125] This is consistent with longstanding case law holding that the prosecution is not required to help the defense collect evidence.[126]

When it will not prejudice the defendant's case to disclose to the state what evidence they are seeking—and in many cases it will prejudice the defendant's

---

117. State v. Bray, 422 P.3d 250, 254 (Or. 2018) (commenting on the fact that the trial court below granted the defendant's "motion to compel the state to use its authority under the [SCA] to obtain [the witness]'s records from Google"); State v. Vasquez, No. 08-16-00089-CR, 2018 WL 4178462, at *5 (Tex. App. Aug. 31, 2018) (commenting on the trial court's decision "to compel the State to obtain and produce 'all information, including but not limited to all photos, posts, messages, and all other information' from Facebook pertaining to a designated Facebook account").

118. It is unclear from the appellate opinion in *State v. Vasquez* whether the state affirmatively requested a warrant and whether that warrant was granted. *Vasquez*, 2018 WL 4178462, at *8 ("The State had no unilateral right to obtain the communications that Vasquez sought. Only a neutral magistrate could have ordered the production of that material. The SCA indeed requires that a governmental entity initiate the request (or here, application for a warrant), but there is nothing in the record that shows the State did not do so.").

119. *Bray*, 422 P.3d at 254.

120. *Id.*

121. *Id.* at 257.

122. *Id.* at 256-57.

123. 373 U.S. 83, 87 (1963) (imposing an absolute obligation on the prosecution to turn over exculpatory evidence within their possession to the defense).

124. OR. REV. STAT. ANN. § 135.815 (West 2022).

125. *Bray*, 422 P.3d at 258 ("When the state cannot obtain documents without judicial assistance, it cannot be said to have power over them.").

126. *See, e.g.*, United States v. Baker, 1 F.3d 596, 598 (7th Cir. 1993) ("Certainly, *Brady* does not require the government to conduct discovery on behalf of the defendant.").

case—it may be worth attempting to cooperate with law enforcement for a warrant. However, if the state refuses, it is unlikely that a court will enforce compliance. There is no statutory basis in the SCA to mandate law-enforcement cooperation with a criminal defendant's request for a search warrant for covered content. The question of whether a criminal defendant has a constitutional right to such law-enforcement cooperation under the Due Process Clause is explored in greater detail in Section IV.A.

3. *Interrogating Online Platforms' Classification as ECS or RCS Providers Under the SCA*

To avoid the SCA's restrictions, criminal defendants might also argue that the provider in question is not covered by the statute. As described in Section II.B, the SCA's prohibitions on disclosure apply to ECS and RCS providers in certain circumstances.[127] The SCA's coverage is specific: if a provider does not fit within either of the two descriptions, then they are not regulated by the SCA.[128] Therefore, if a criminal defendant could show that the online platform they sought to subpoena is not an ECS or RCS provider, then that company could not invoke the SCA to block the defendant's subpoena.

While there are strong statutory-interpretation arguments that the companies most frequently involved in SCA litigation with criminal defendants do *not* fall under the SCA, this strategy poses challenges insofar as courts have largely refrained from questioning the assumption that such companies are covered.[129]

---

127. 18 U.S.C. § 2702(a)-(b) (2018).

128. *See* Flagg v. City of Detroit, 252 F.R.D. 346, 349 (E.D. Mich. 2008) ("As is evident from these provisions, the prohibitions set forth in § 2702(a) govern service providers to the extent that they offer either of two types of services: an 'electronic communications service' or a 'remote computing service.'"); *In re* JetBlue Airways Corp. Priv. Litig., 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005) (finding that where plaintiffs did not establish the defendant company constituted an ECS or RCS provider as defined by the statute, the company "as a matter of law is not liable under § 2702 of the ECPA"); *see also* Kerr, *supra* note 93, at 1213 ("If the provider fits within the two categories, the SCA protects the communication; otherwise, only Fourth Amendment protections apply.").

129. *See, e.g.*, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 412 (Cal. 2020) (Cuéllar, J., concurring) ("Courts—including our own—have nonetheless assumed that social media entities such as Facebook are regulated by the SCA." (citing Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725 (Cal. 2018))); *Hunter*, 417 P.3d at 740 ("Prior decisions have found that Facebook and Twitter qualify as either an ECS or RCS provider and hence are governed by section 2702 of the SCA. All parties assume the same with respect to all three providers before us. We see no reason to question this threshold determination." (footnote omitted)).

The San Diego County District Attorney's office has effectively laid out the argument that the SCA does not apply to Facebook in an intervenor brief submitted in the *Touchstone* litigation.[130]

With regards to ECS providers, the SCA mandates that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[131] The San Diego County District Attorney's office argued that this provision does not apply to Facebook because the site is not holding content in electronic storage as defined by the statute.[132] Specifically, electronic storage is limited to "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication . . . for purposes of backup protection of such communication."[133] As the San Diego County District Attorney's office explained, this definition reflects how emails were sent between dial-up service providers at the time the statute was drafted, but cannot be read to encompass how Facebook operates today.[134] Facebook does not serve as a mere conduit or intermediary for users' information in the same way that email servers originally did; it has its own rights to and engagement with that information. Indeed, Facebook has a license over the content users upload.[135] To the extent that Facebook retains data, it is for the company's own purposes, not simply for the purposes of backup protection as described in the statute. Facebook reviews and

130. San Diego County District Attorney Intervenor Brief, *supra* note 101, at 1. The California Supreme Court resolved the case on other grounds. *See Touchstone*, 471 P.3d at 403 ("We will not assess the underlying merits of the business model thesis. Yet we observe that, contrary to Facebook's view, we have not determined that Facebook is a provider of either ECS or RCS under the Act."). However, two concurring justices highlighted that the question deserved further attention. *Id.* at 403-04 (Cantil-Sakauye, C.J., concurring); *id.* at 411 (Cuéllar, J., concurring).

131. 18 U.S.C. § 2702(a)(1) (2018).

132. San Diego County District Attorney Intervenor Brief, *supra* note 101, at 4-6.

133. 18 U.S.C. § 2510(17) (2018).

134. San Diego County District Attorney Intervenor Brief, *supra* note 101, at 9, 15.

135. *See Terms of Service*, FACEBOOK (Oct. 22, 2020), https://www.facebook.com/terms.php?ref=pf [https://perma.cc/Y7W2-VZNH] ("[W]hen you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content . . . ."); *see also* San Diego County District Attorney Intervenor Brief, *supra* note 101, at 10.

analyzes user data to improve its products and to generate revenue through advertisements.[136] For that reason, Facebook does not store communications in a way that is "incidental to the electronic transmission thereof" or "for purposes of backup protection of such communication."[137] Instead, Facebook's storage and use of information is central to its business model.

The San Diego County District Attorney's office also addressed why Facebook does not qualify for SCA coverage as an RCS provider. The statute dictates that RCS providers

> shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing . . . .[138]

As described above, Facebook uses "what you share and do on . . . our Products" both to improve their products and to generate advertising revenue.[139] Facebook therefore *is* authorized to access the content of communications on its website for purposes beyond storage or computer processing. In fact, the company has explicitly confirmed that it uses the content on its site for those purposes.[140]

---

136. *See* FACEBOOK, *supra* note 134 ("We use the data we have — for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products — to personalize your experience."); *id.* ("We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you."); *see also* San Diego County District Attorney Intervenor Brief, *supra* note 101, at 11-12.

137. 18 U.S.C. § 2510(17) (2018).

138. *Id.* § 2702(a)(2).

139. *See Terms of Service*, *supra* note 134.

140. Facebook CEO Mark Zuckerberg testified to this in Senate hearings:

> What we allow is for advertisers to tell us who they want to reach, and then we do the placement. So, if an advertiser comes to us and says, "All right, I am a ski shop and I want to sell skis to women," then we might have some sense, because people shared skiing-related content, or said they were interested in that, they shared whether they're a woman, and then we can show the ads to the right people without that data ever changing hands and going to the advertiser.

Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on Com., Sci., & Transp. and the S. Comm. on the Judiciary, 115th Cong. 42 (2018) (statement of Mark Zuckerberg); *see also* San Diego County District Attorney Intervenor Brief, supra note 101, at 12 (quoting Zuckerberg's testimony).

Instagram, which shares information with Facebook and is owned by the same parent company,[141] retains comparable rights to content users post to its website and therefore could be similarly excluded from the reach of the SCA.[142] The same is true of Twitter.[143] In fact, the business model of modern online platforms that do not charge for their services—which includes most social-media companies—is premised on data mining users' content.[144] This data-mining business model removes these companies from the parameters of ECS and RCS providers as defined by the statute, and therefore the SCA's prohibitions on disclosure should not apply to them.

This line of reasoning could arguably even apply to companies that more closely resemble the more traditional email providers that the drafters of the SCA had in mind.[145] For example, Google, which operates Gmail and numerous other products, "do[es] not process email content to serve ads," but "conduct[s] automatic processing of emails" to deliver its "world-class safety features" and reads

---

141. Facebook, Instagram, and a number of other social-media applications were subsumed under the parent company Meta Platforms, Inc. in October 2021. *Introducing Meta: A Social Technology Company*, META (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta [https://perma.cc/JK2Z-47N7].

142. *See Terms of Use*, INSTAGRAM (Dec. 20, 2020), https://help.instagram.com/581066165581870 [https://perma.cc/9VC9-NL8X].

143. *See Twitter Terms of Service*, TWITTER (Aug. 19, 2021), https://twitter.com/en/tos [https://perma.cc/N5PU-ZVE8] ("By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content . . . . You agree that this license includes the right for Twitter to provide, promote, and improve the Services and to make Content submitted to or through the Services available to other companies, organizations or individuals for the syndication, broadcast, distribution, Retweet, promotion or publication of such Content . . . .").

144. *See, e.g., Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, AMNESTY INT'L (Nov. 21, 2019), https://www.amnesty.org/en/wp-content/uploads/2021/05/POL3014042019ENGLISH.pdf [https://perma.cc/4DQ9-X57Z].

145. Courts have generally found that email providers are covered by the SCA. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008), *rev'd and remanded on other grounds sub nom.* Ontario v. Quon, 560 U.S. 746 (2010); Theofel v. Farey-Jones, 359 F.3d 1066, 1075-76 (9th Cir. 2003). However, at least one court has held that an individual's web-based Yahoo! Mail account was not covered by the SCA because Yahoo! was not retaining the content for the purposes of backup protection. Jennings v. Jennings, No. 07-CP-40-1125, 2008 WL 8185934 (S.C.C.P. Sept. 23, 2008). For more information on this split over the applicability of the SCA to email providers, see Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 48-53 (2015).

emails beyond this automatic process "for security purposes, such as investigating a bug or abuse."[146] Google requires users to provide the company with a license to their content, which the company uses to "customize [its] services for [users], such as providing recommendations and personalized search results, content, and ads."[147] While Google's authority to use the content of emails is distinct from the authority social-media companies like Facebook, Instagram, and Twitter retain through their terms of service, it still goes beyond the type of access contemplated for ECS and RCS providers in the SCA. Criminal defendants may therefore advance this argument in the case of any company that uses the content of communications to improve its products, tailor its advertisements, or to further its business model in other ways.

The lack of alignment between online platforms' current business practices and covered providers under the SCA offers a strong statutory argument as to why criminal defendants should be able to access the content of electronic communications on these platforms. Nonetheless, defendants seeking to advance this argument will encounter hurdles. To date, no court has held that any of the companies listed above fall outside the parameters of the SCA. On the contrary, the majority of courts encountering the issue in either the criminal or civil context have held or assumed that such companies are either ECS or RCS providers.[148] While there have been some discrepancies as to the specifics of that analysis (for example, whether certain companies qualify as ECS or RCS providers), all courts that have directly confronted the question have "uniformly concluded that communications sent to social-media platforms or even private websites are clearly 'electronic communications' under the federal act."[149]

However, defendants have typically failed to raise the question of whether the social-media company they seek information from is actually covered by the SCA, and many courts have simply assumed that the company is covered without investigating the statutory language.[150] Moreover, no court has yet addressed the business-model theory advanced by the San Diego County District Attor-

146. Suzanne Frey, *Ensuring Your Security and Privacy Within Gmail*, GOOGLE (July 3, 2018), https://www.blog.google/technology/safety-security/ensuring-your-security-and-privacy-within-gmail [https://perma.cc/G5AC-JTAT].

147. *Google Terms of Service*, GOOGLE (Mar. 31, 2020), https://policies.google.com/terms?hl=en-US [https://perma.cc/U24T-VPT6].

148. *See, e.g.*, State v. Johnson, 538 S.W.3d 32, 68-69 (Tenn. Crim. App. 2017) (collecting cases that conclude that the SCA applies to social-media sites).

149. *In re* Application of State for Commc'ns Data Warrants to Obtain the Contents of Stored Commc'ns from Twitter, Inc., 154 A.3d 169, 177 (N.J. Super. Ct. App. Div. 2017); *see also Johnson*, 538 S.W.3d at 68-69.

150. *See* cases cited *supra* note 129.

ney's Office, which argues that companies whose terms of service grant the company legal rights to their users' communication content and who share their users' data with third parties are excluded from the statute.[151] Insofar as it would exempt huge swathes of previously protected content from the SCA, this theory also raises concerns related to privacy and legislative intent that may make courts hesitant to change course. Nonetheless, that is an issue that counsels in favor of revising the outdated legislation to adequately protect users' privacy, not twisting its words to accommodate online platforms that are clearly beyond its scope.

This argument is worth pursuing as a potential pathway to information disclosure.[152] But the fact that no court has found that social-media companies are not providers as covered by the SCA, and that existing jurisprudence has held the opposite, indicates that this theory cannot be relied upon to give defendants access to evidence.

B. Statutory Litigation Strategies: Exceptions to the SCA

For the reasons described above, circumventing subpoenas to online platforms may not always be possible. There are limited scenarios in which defendants can subpoena covered ECS and RCS providers for the contents of electronic communications. To date, the only avenue courts have recognized for allowing defense counsel to access the content of electronic communications directly through covered providers is through the exceptions to the SCA.

Courts in SCA litigation have recognized exceptions for (1) disclosure to an addressee or intended recipient and (2) disclosure with consent.[153] While these exceptions may prove helpful in some circumstances, they are narrowly applied.

1. Exception for Addressee or Intended Recipient

The first exception to § 2702(a)'s bar on disclosure of the contents of communications indicates that providers "may divulge the contents of a communication . . . to an addressee or intended recipient of such communication."[154]

---

151. *See* Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 411 (Cal. 2020) (Cuéllar, J., concurring) (suggesting that courts ought to take up this "crucial matter").

152. To the extent that courts reach a conclusion that modern social-media companies are *not* covered by the SCA, new legislation would be necessary to adequately protect users' privacy interests. Any such statute could include a symmetrical savings provision to "maintain the status quo investigative powers of both law enforcement and defense counsel." *See* Wexler, *supra* note 9, at 259.

153. The other exceptions would not apply to criminal defendants and are therefore not considered in this Section.

154. 18 U.S.C. § 2702(b)(1) (2018).

When the defendant is an addressee or intended recipient of the communication they seek, this exception provides a helpful avenue because the defendant does not need to involve third parties like senders or recipients; they can issue the subpoena directly to the online platform themselves. But precisely for that reason, there are only a limited number of scenarios where this exception would be useful. If the defendant was an addressee or intended recipient of the communication, they may still have access to the content themselves, eliminating the need to seek it from the online platform. Instead, defendants are more likely to seek the content of communications involving a witness, alleged victim, or some other third party. In those scenarios this exception will not apply.

This exception will be useful in circumstances where the defendant no longer has access to the account where they received the communication or cannot access the communication itself. With regards to the latter, some forms of social-media communications automatically disappear after they have been viewed or after a set amount of time has expired.[155] In *Facebook, Inc. v. Pepe*, the D.C. Court of Appeals became the first court to consider whether the intended-recipient exception covered these forms of disappearing content.[156] The defendant in the case faced criminal charges after shooting a man and sought to support his self-defense theory by obtaining a disappearing Instagram story he had received from the alleged victim. Facebook (which at the time owned Instagram) argued that the effervescent nature of an Instagram story made the defendant "a *former* addressee" as opposed to one covered by the SCA, and by extension, "that a receiver must have *current* access to a communication when seeking its disclosure."[157] If adopted, this current-access requirement would eviscerate any utility of the exception for addressees or intended recipients, as there would be no need to obtain it via a subpoena. The court ultimately determined that "[i]n the ordinary sense of the term, being an 'addressee or intended recipient' of a communication is not linked in any way to how long the receiver continues or is intended to

155. Snapchat and Instagram stories serve as examples of popular self-deleting content. *See Snapchat Support: When Does Snapchat Delete Snaps and Chats?*, SNAPCHAT, https://support.snapchat.com/en-US/article/when-are-snaps-chats-deleted [https://perma.cc/89RA-LLHQ] ("Snapchat servers are designed to automatically delete all Snaps after they've been viewed by all recipients. . . . Snapchat servers are designed to automatically delete messages sent in one-on-one Chat after both Snapchatters have opened and left the Chat. . . . Snapchat servers are designed to automatically delete Snaps you add to your Story 24 hours after you added them."); *When Does My Instagram Story Disappear?*, INSTAGRAM (2022), https://www.facebook.com/help/instagram/1729008150678239 [https://perma.cc/YL9N-4DEB] ("Photos and videos you share to your story disappear from Feed, your profile and Direct after 24 hours, unless you add it as a highlight.").

156. 241 A.3d 248, 253-54 (D.C. 2020).

157. *Id.* at 255.

possess it," and therefore affirmed the lower court's ruling by holding Facebook in contempt and denying the company's motion to quash.[158]

The intended-recipient exception can therefore be useful to defendants seeking communications to which they no longer have access themselves, either because of a built-in automatic disappearing feature of the content (i.e., defendants attempting to access expired Snapchat or Instagram stories) or for any other reason. In cases where the communication was between third parties, it will not provide a fruitful avenue for access.

2. *Exception Based on Consent*

Another exception to the SCA allows providers to disclose content with the "consent of the originator or an addressee or an intended recipient."[159] This exception has been invoked in cases involving various conceptions of consent, which can be understood as affirmative consent, implied consent, and compelled consent.

Affirmative consent refers to situations in which the sender or recipient of an electronic communication affirmatively and voluntarily grants their permission for ECS providers to disclose the contents of their communications. This form of consent may be of use in scenarios where defendants can secure consent themselves, but will likely not be possible in scenarios in which third parties have adverse interests to the defendant. Additionally, there is no clear standard to determine who is authorized to give consent and what they must prove to do so, further limiting the utility of this strategy for criminal defendants. In one case, a defendant served a subpoena on Microsoft and Yahoo to obtain the contents of his *own* emails upon his consent.[160] The providers refused to honor the subpoena unless the defendant provided identifying information including the passwords for his accounts, which he could no longer remember after being incarcerated for years pending his trial.[161] Such a high bar creates barriers for criminal defendants seeking access to content through this exception.

Implied consent arises in cases where the sender or recipient of a communication has not offered their affirmative consent for the online platform to disclose

---

158. *Id.*

159. 18 U.S.C. § 2702(b)(3) (2018).

160. *See* United States v. Amawi, 552 F. Supp. 2d 679, 680 (N.D. Ohio 2008).

161. *Id.* This is not the only case where a court has "accept[ed] an [ISP's] contention that it lacks reliable means to verify proper consent" where a defendant sought content from their own account. *See* United States v. Wenk, 319 F. Supp. 3d 828, 829 n.2 (E.D. Va. 2017). The difficulties of establishing consent and meeting the high threshold imposed by online platforms further limits the usefulness of this statutory exception even in cases where it is applicable to content a defendant is seeking.

content pursuant to a subpoena, but has nonetheless consented in some other way. For example, social-media account holders may consent to the disclosure of their information by configuring their posts as public.[162] At least one defendant has unsuccessfully argued that this exception should also extend to posts sent to a large group of friends or followers, on the theory that the latter is effectively public insofar as it can be shared widely by other users.[163] This exception has been held to cover content that remains configured as public at the time of the subpoena, but no court has yet decided whether this same exception would apply to content that was originally posted publicly but was either restricted or deleted before the issuance of the subpoena.[164] Facebook has argued:

> [T]he SCA protects electronic communications that were previously public but are private at the time the discovery is sought. Revocation of consent is a well-recognized doctrine in the law, and there are strong policy reasons for applying it in circumstances where a person modifies the privacy settings of a post to make it non-public.[165]

Such a holding would limit the reach of this exception, especially given that posts that are contemporaneously configured to be public are by definition accessible to the defendant without a subpoena.

Finally, compelled consent may arise in cases where the court orders individuals to consent to the disclosure of covered content for the express purpose of bringing such content within this exception to the SCA. This route has been pursued in civil SCA cases[166] but has not yet arisen in a criminal SCA case.

---

162. *See* Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 744 (Cal. 2018).

163. *See id.* at 728.

164. *See id.* at 753; *see also* Brendan Sasso, *Digital Due Process: The Government's Unfair Advantage Under the Stored Communications Act*, 8 VA. J. CRIM. L. 35, 53 (2020) (explaining that the *Hunter* court "left open the question of whether consent under the SCA is revocable").

165. Petitioner's Supplemental Brief Addressing the Effect of *Facebook, Inc. v. Superior Court* (*Hunter*) at 2, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203).

166. *See, e.g.*, Flagg v. City of Detroit, 252 F.R.D. 346, 355 (E.D. Mich. 2008) ("[I]t is immaterial whether a party, such as the City here, might prefer not to give the necessary consent—if a party has the requisite control over a requested document, it must exercise this control in order to comply with the mandate of Rule 34 [of the Federal Rules of Civil Procedure]."); Negro v. Superior Ct., 179 Cal. Rptr. 3d 215, 222 (Ct. App. 2014) ("[W]here users are also parties to civil litigation, the court has the means to *compel* them to *give* their actual consent."); Juror No. One v. Superior Ct., 142 Cal. Rptr. 3d 151, 153 (Ct. App. 2012). Complications may arise in attempts to compel consent from account holders who are not parties to the case. For further discussion of compelled consent, see Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1059-61 (2014).

3. *Outcome of Exceptions: Permissive Versus Mandatory Disclosure*

One limitation to the exceptions-based approach to disclosure comes from the statutory language in § 2702(b). This provision introduces all of the exceptions to § 2702(a)'s prohibitions on disclosure and indicates that "provider[s] described in subsection (a) *may* divulge the contents of a communication" in accordance with certain enumerated circumstances.[167] Based on this language, online platforms have argued that the exceptions allow only for permissive disclosure at their own discretion.[168]

Courts interpreting the SCA in the civil context were the first to confront the question of whether the exceptions listed in § 2702(b) required permissive or mandatory disclosure, and many sided with the online platforms and found the former.[169] Since then, the few criminal courts considering the issue have split on the question of whether the statute requires mandatory or permissive disclosure pursuant to a lawfully ordered subpoena. In *United States v. Wenk*, the District Court for the Eastern District of Virginia held that "[b]ased upon the plain language of the SCA, service providers such as Google are not required to disclose communications covered by the Act, even when the relevant consent is properly given. Instead, the SCA vests service providers with discretionary authority to disclose once consent is properly given."[170] On the other hand, the highest courts in the District of Columbia and California have concluded that subpoenas issued pursuant to a SCA exception require mandatory disclosure, for reasons detailed below.[171]

Given the small number of criminal courts to consider this issue and the conflicting opinions of the ones that have, the question of whether exceptions under

---

167. 18 U.S.C. § 2702(b) (2018) (emphasis added).

168. Facebook Supplemental Letter Brief to the Court of Appeal at 1-7, *Touchstone*, 471 P.3d 383 (No. S245203).

169. *See, e.g.*, Schweickert v. Hunts Point Ventures, Inc., No. 13-cv-675, 2014 WL 6886630, at *13 (W.D. Wash. Dec. 4, 2014) ("Even if the Court could compel Plaintiff to consent to the disclosure of some [of] her emails under Rule 34, the providers would still only be permitted, but not required, to turn over the contents under 18 U.S.C. § 2702(b)(3)."). *But see Negro*, 179 Cal. Rptr. 3d at 231-32 (interpreting § 2702(b) to require mandatory disclosure for subpoenas issued pursuant to a statutory exception).

170. 319 F. Supp. 3d 828, 829 (E.D. Va. 2017) (footnote omitted).

171. Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 752 (2018) ("[I]f Congress intended to preclude a state from enforcing a nongovernmental entity's civil or criminal subpoena that is lawful under state law (and as to which the federal statute does not preclude disclosure), such a prohibition would have been made clear in the Act. We find no intent by Congress to preempt state law in this setting."), *cert. denied*, 140 S. Ct. 2761 (2020); Facebook, Inc. v. Pepe, 241 A.3d 248, 258 (D.C. 2020) (quoting *Hunter*, 417 P.3d at 751).

§ 2702(b) lead to mandatory or permissive disclosure remains open. In accordance with the decisions of the high courts of the District of Columbia and California, I suggest that disclosure pursuant to an exception should be held to be mandatory according to traditional rules of statutory interpretation. While linguistic canons of statutory interpretation frequently interpret the use of the term "may" in a precatory or discretionary manner, this is generally in contrast to the term "shall."[172] Further, the implication that "may" implies discretion "is by no means invariable . . . and can be defeated by indications of legislative intent to the contrary or by obvious inferences from the structure and purpose of the statute."[173] Both are present here. The SCA contrasts "may" with "shall not."[174] As one California court considering this issue found,

> [T]he subdivision where "may" appears is framed not as a grant of discretionary power . . . but as a special exception to a general prohibition. In such a context all "may" means is that the actor is excused from the duty, liability, or disability otherwise imposed by the prohibition.[175]

Moreover, there is no evidence in the legislative history to "categorically immunize[] service providers against compulsory civil process where the disclosure sought is excepted on other grounds from the protections afforded by the Act."[176] A finding that the SCA does immunize service providers would apply more broadly than just to compulsory civil process, given that the exceptions in § 2702(b) also govern the disclosure of communications to government entities as authorized in § 2703, as well as disclosure "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A . . . ."[177] There is no indication that the drafters sought to give companies like Facebook and Google discretion over whether to comply with investigations by the National Center for Missing and Exploited Children or by law enforcement more generally. Defendants therefore have a strong case for mandatory disclosure should their subpoena fall under one of the exceptions. However, to the extent that there is contrary case law, defendants may be unsuccessful in pursuing content under the exceptions.

---

172. William N. Eskridge, Jr. & Philip P. Frickey, *Foreword: Law as Equilibrium*, 108 HARV. L. REV. 26, 98 (1994).

173. United States v. Rodgers, 461 U.S. 677, 706 (1983).

174. 18 U.S.C. § 2702(a)-(b) (2018).

175. Negro v. Superior Ct., 179 Cal. Rptr. 3d 215, 232 (Ct. App. 2014).

176. *Id.* at 233.

177. 18 U.S.C. § 2702(b)(6) (2018); *see also* Facebook, Inc. v. Pepe, 241 A.3d 248, 258 (D.C. 2020) ("[S]ome of the excepted circumstances in which subsections (b) and (c) say a provider 'may divulge' information are, in fact, circumstances in which the provider *must* divulge it.").

IV. CONSTITUTIONAL CHALLENGES TO THE SCA

Courts and online platforms have often suggested that defendants' avenues to access evidence described above eliminate the need for defendants to be able to subpoena ECS or RCS providers for content.[178] In some cases, this may well be true. But of the court opinions dealing with defendants who face the SCA as a barrier to accessing evidence reviewed for this study, this is only true in *two* cases. The D.C. Court of Appeals held that a defendant could access electronic communications pursuant to the intended-recipient exception in § 2702(b).[179] Similarly, the Supreme Court of California held that a defendant could access information under the consent exception, assuming that he met other subpoena requirements.[180] All other criminal court opinions have denied defendants access to information at least in part because of the limitations imposed by the SCA.[181] This suggests that the SCA places a significant barrier between criminal defendants and potentially exculpatory evidence to which they are constitutionally entitled.

The jurisprudence blocking criminal defendants from accessing exculpatory evidence is in part rooted in the fact that a significant portion of SCA case law developed in the context of civil litigation.[182] The rights of civil litigants to access evidence are weaker than the rights of criminal defendants, given the stronger interests in liberty and life that can be put at stake in criminal proceedings compared to the property interests that are at issue in both criminal and civil proceedings.[183] Despite these constitutional differences, courts have largely transposed SCA interpretations that emerged in the civil context wholesale into the

178. *See supra* notes 99-102.

179. *Pepe*, 241 A.3d at 258.

180. Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 728-29 (Cal. 2018), *cert. denied*, 140 S. Ct. 2761 (2020).

181. *See* United States v. Amawi, 552 F. Supp. 2d 679, 680-81 (N.D. Ohio 2008); United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015); United States v. Wenk, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017); United States v. Meintzschel, No. 20-CR-00023-FL-1, 2020 WL 7340017, at *3 (E.D.N.C. Dec. 14, 2020); People v. Q.H., No. A142771, 2016 WL 5118287, at *13 (Cal. Ct. App. Sept. 21, 2016); Facebook, Inc. v. Wint, 199 A.3d 625, 629 (D.C. 2019); R.C. v. Chilcoff, No. SJ-2020-008, 2020 WL 8079734, at *6 (Mass. Dec. 15, 2020); State v. Bray, 422 P.3d 250, 259 (Or. 2018); State v. Johnson, 538 S.W.3d 32, 69 (Tenn. Crim. App. 2017); State v. Vasquez, No. 08-16-00089-CR, 2018 WL 4178462, at *7-8 (Tex. Ct. App. Aug. 31, 2018).

182. *See, e.g.*, Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2736-37 (2021) (citing O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72 (Ct. App. 2006)).

183. *See, e.g.*, M.L.B. v. S.L.J., 519 U.S. 102, 139-40 (1996) (Rehnquist, C.J., dissenting).

criminal context.[184] This importation is at least in part to blame for the poor fit between SCA jurisprudence and the constitutional rights of criminal defendants.

As detailed in Part III, there are some circumstances in which a defendant will need to subpoena covered ECS or RCS providers for information where none of the statutory exceptions apply. I argue that to the extent that the SCA would bar disclosure of exculpatory evidence in these circumstances, it is unconstitutional. By preventing defendants from accessing potentially exculpatory information—information that *is* available to the prosecution—the SCA infringes on the "area of constitutionally guaranteed access to evidence" created under Fifth, Sixth, and Fourteenth Amendment jurisprudence.[185]

Numerous defendants have raised constitutional challenges to denials of evidence pursuant to the SCA.[186] Courts have generally avoided these constitutional questions by resolving cases on statutory grounds,[187] or by suggesting defendants should pursue the information they seek through an avenue that is not covered by the SCA.[188] However, some courts have alluded to the possibility of constitutional issues with the SCA, noting that "the SCA might eventually need to be declared unconstitutional to the extent it precludes enforcement of such a trial subpoena issued by the trial court itself, or by defendants, with production to the court,"[189] or that "in a given case the limitations imposed by the SCA could impermissibly interfere with a criminal defendant's right to compulsory process."[190] Defendants in such a position should argue—and reviewing courts should hold—that the SCA is unconstitutional as applied to their circumstances.

This Part explores potential challenges to the SCA grounded in the U.S. Constitution.[191] The specific circumstances of a defendant may counsel in favor of

184. *See* Wexler, *supra* note 182, at 2737.

185. United States v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982).

186. *See, e.g.*, *Pierce*, 785 F.3d at 841; Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 387 (Cal. 2020); Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 728 (Cal. 2018), *cert. denied*, 140 S. Ct. 2761 (2020); Facebook, Inc. v. Pepe, 241 A.3d 248, 253 n.7 (D.C. 2020).

187. *See, e.g.*, *Touchstone*, 471 P.3d at 402; *Pepe*, 241 A.3d at 253 n.7.

188. *See, e.g.*, *Pierce*, 785 F.3d at 842; Facebook v. Wint, 199 A.3d 625, 628-29 (D.C. 2019).

189. *Hunter*, 417 P.3d at 735 (emphasis omitted).

190. *Wint*, 199 A.3d at 633.

191. State constitutions and law may offer additional context-specific support for challenges to the SCA. Challenges grounded in state law are beyond the scope of this Note, but as an example, the discovery obligations that the California Penal Code imposes on prosecutors are more expansive than materials covered by federal *Brady* requirements, *see* CAL. RULES OF PRO. CONDUCT r. 5-110 n.3 (CAL. ST. BAR 2017), while the California Constitution provides an independent state constitutional ground for criminal reciprocal discovery rights, CAL. CONST. art. I, § 30(c). Other states may similarly have constitutional and other bodies of law that rise above the floor of criminal defendants' constitutional rights set by the U.S. Constitution.

particular interpretations of these arguments or additional constitutional arguments not included below.

A. Due-Process Rights

The Due Process Clauses in the Fifth and Fourteenth Amendments prohibit the deprivation of "life, liberty, or property, without due process of law."[192] Due-process rights apply to criminal defendants facing both state and federal prosecutions. In the criminal context, the Supreme Court has held that due process requires "the right to a fair opportunity to defend against the State's accusations."[193] This due-process right manifests in a variety of protections for criminal defendants, including rights that relate directly to a defendant's ability to access and present exculpatory evidence. Criminal defendants' due-process rights to evidence have developed under several different theories: (1) protection from prosecutorial misconduct through *Brady v. Maryland* and its progeny;[194] (2) *Wardius v. Oregon*'s mandate of reciprocal discovery;[195] and (3) the protection of individuals who are "actually innocent" from punishment. While this case law is complex and balances a number of distinct considerations, each line of cases is motivated by a fundamental concern with the accuracy of criminal proceedings. As the Supreme Court has explained, "constitutional privileges deliver[] exculpatory evidence into the hands of the accused, thereby protecting the innocent from erroneous conviction and ensuring the integrity of our criminal justice system."[196] The due-process right to evidence — motivated by the fundamental concern with the accuracy of criminal proceedings — provides a constitutional basis for the disclosure of evidence covered by the SCA.

1. Brady *and Prosecutorial Misconduct*

Brady v. Maryland provided criminal defendants with perhaps the most well-known and well-established due-process right to evidence. In *Brady*, the Supreme Court held that the "suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution."[197] In other words, *Brady* imposed an absolute obligation on the

192. U.S. CONST. amends. V, XIV, § 1.

193. Chambers v. Mississippi, 410 U.S. 284, 294 (1973).

194. 373 U.S. 83, 87 (1963).

195. 412 U.S. 470 (1973).

196. California v. Trombetta, 467 U.S. 479, 485 (1984).

197. *Brady*, 373 U.S. at 87.

prosecution to turn over material evidence within their possession to the defense. Subsequent cases have affirmed a criminal defendant's due-process right to *Brady* material.[198]

The *Brady* line of cases prohibiting prosecutorial misconduct in the form of withholding evidence is informed by both a procedural motive to ensure a fair trial[199] and a related substantive motive to obtain accurate results.[200] As the Supreme Court explained in *United States v. Bagley*, "[t]he *Brady* rule is based on the requirement of due process. Its purpose is not to displace the adversary system as the primary means by which truth is uncovered, but to ensure that a miscarriage of justice does not occur."[201] Both the procedural and substantive elements of *Brady* are evident in the test that courts employ to determine whether a *Brady* violation has occurred: a criminal defendant seeking relief from a failure to disclose under *Brady* must show prejudice, or more specifically, "that 'there is a reasonable probability' that the result of the trial would have been different if the suppressed documents had been disclosed to the defense."[202] While this test largely implicates the accuracy of the conviction, the Supreme Court also looks to procedural benchmarks. For example, if *Brady* material was withheld, the Court will consider "whether in its absence [the defendant] received a fair trial, understood as a trial resulting in a verdict worthy of confidence."[203]

Brady and its progeny have frequently served as a basis for arguments that criminal defendants must be allowed access to evidence derived from forms of emerging technology.[204] This is likely because prosecutors are often granted access to the fruits of these emerging technologies before criminal defendants (if criminal defendants are ever granted access), and *Brady* provides a channel to obtain evidence possessed by prosecutors.

As discussed above in Section III.A, online platforms have proposed a *Brady*-like remedy to the challenges the SCA poses for criminal defendants attempting to access social-media evidence. This would effectively impose an obligation on

198. *See, e.g.*, Giglio v. United States, 405 U.S. 150 (1972).

199. *See Brady*, 373 U.S. at 87 ("Society wins not only when the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly.").

200. *See* United States v. Bagley, 473 U.S. 667, 675 (1985).

201. *Id.*

202. Strickler v. Greene, 527 U.S. 263, 289 (1999).

203. Kyles v. Whitley, 514 U.S. 419, 434 (1995).

204. *See, e.g.*, Fairfield & Luna, *supra* note 166, at 1030-31; Rebecca Darin Goldberg, Note, *You Can See My Face, Why Can't I? Facial Recognition and* Brady, 5 COLUM. HUM. RTS. L. REV. ONLINE 261 (2021), http://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-and-brady [https://perma.cc/BRF9-26W8]; Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180 (2020).

the prosecution to disclose exculpatory evidence from covered ECS and RCS providers. However, a fatal limitation to the applicability of the *Brady* doctrine to content covered by the SCA is that the relevant contents of electronic communications are in the possession of the online platforms, not the government.

While prosecutors "ha[ve] a duty to learn of" material evidence known internally and to anyone "acting on the government's behalf in the case," *Brady* imposes no obligation or expectation that prosecutors go beyond that threshold.[205] This means that if a criminal defendant seeks evidence that the prosecution has not pursued—for example, impeachment evidence for a government witness, corroborating records to support an alibi, or other evidence that is not necessarily relevant to the government's affirmative case—*Brady* does not impose any obligation on the government to obtain that information. In such circumstances, the prosecution is not obscuring or withholding information, and under existing case law is not engaging in prosecutorial misconduct.[206] Evidence in the possession of online platforms therefore largely remains out of reach from *Brady*'s protections.

Despite the incongruities between evidence covered by traditional *Brady* jurisprudence and the content implicated by the SCA, there is some precedent in access-to-evidence cases for exploring "the extent to which the Due Process Clause imposes on the government the additional responsibility of guaranteeing criminal defendants access to exculpatory evidence beyond the government's possession."[207] In an amicus brief filed on behalf of a criminal defendant seeking access to evidence covered by the SCA, California Attorneys for Criminal Justice suggested an analogy between requiring prosecutors to exercise their SCA search-warrant powers to assist criminal defendants and the practice of requiring the government to provide a defense witness immunity under 18 U.S.C. § 6002.[208] This federal "use-immunity" statute creates an imbalance similar to the asymmetry of the SCA in that it allows prosecutors the ability to grant immunity to a witness in order to secure evidence for the government, but it does not give a comparable opportunity to the defense to seek judicial immunity for witnesses. As the Ninth Circuit observed,

---

205. *Kyles*, 514 U.S. at 437; *see also* Sasso, *supra* note 164, at 47-48 ("If the evidence is not yet in the government's possession, the prosecution has no *Brady* obligation to go find it and provide it to the defense.").

206. *See, e.g.*, United States v. Baker, 1 F.3d 596, 598 (7th Cir. 1993) ("Certainly, *Brady* does not require the government to conduct discovery on behalf of the defendant.").

207. California v. Trombetta, 467 U.S. 479, 486 (1984).

208. *See* Supplemental Brief of Amicus Curiae California Attorneys for Criminal Justice on Behalf of Real Party in Interest Lance Touchstone at 14, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203).

> Faced with repeated claims of the unfairness visited on proceedings in which the defense could make a showing that a witness was likely to have compelling defense evidence assuming that specific predicates were established, a minority of the Federal circuits have found that where the right to a fair trial is at issue . . . [there is a constitutional] basis from a Federal District Court for an order commanding the Government to provide a given witness use immunity. And assuming the appropriate predicate, the government's refusal to grant immunity may amount, on review, to a violation of due process, and under some circumstances to prosecutorial misconduct warranting reversal.[209]

Under this argument, a court could order the prosecution to issue a search warrant to vindicate a criminal defendant's due-process rights.

While arguably worthwhile given the high stakes of criminal proceedings, seeking a *Brady*-like due-process right that would require the government to actively seek out evidence may be an uphill battle. Judges will be reluctant to require the prosecution to use its own investigation powers on behalf of a defendant due to separation-of-powers concerns.[210] Moreover, to successfully make a claim of a *Brady* violation, a defendant would have to establish that the evidence would have resulted in a different outcome. This is a high standard to meet and is based on a fact-specific inquiry. It is impossible to say whether the contents of electronic communications *generally* satisfy this standard, but it seems plausible that in some cases exculpatory evidence contained on social media would rise to this level.

Despite its inherent weaknesses, this *Brady* argument may be worth pursuing in cases where a defendant has limited means to access the content of electronic communications. Even if a defendant cannot establish that prosecutors have an obligation under the Due Process Clause to secure the contents of communications in the possession of online platforms, which may well be the case, *Brady*'s roots in the importance of accuracy to a criminal proceeding may still be helpful to criminal defendants seeking evidence. While protection from prosecutorial misconduct may not provide defendants a direct pathway to evidence, the underlying due-process jurisprudence that led to *Brady* and its progeny could

---

209. *Id.* at 14-15 (citing United States v. Straub, 538 F.3d 1147, 1157-59 (9th Cir. 2008)).

210. *See EPCA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Const., C.R., & C.L. of the H. Comm. on the Judiciary*, 111th Cong. 128 (2010) (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP) (observing that "[j]udges, for their part, can be reluctant based on separation of power issues to require the government to use its investigative powers at the behest of a defendant to retrieve the [electronic] materials" held by online platforms); *see also* Sasso, *supra* note 164, at 62 ("It seems unlikely that many judges would be comfortable commandeering the warrant process to help a defendant gather evidence.").

be invoked by analogy to support a defendant's right to access exculpatory evidence in other contexts. *Brady* has provided courts an opportunity to expound upon the values of accuracy in criminal proceedings, which constitute a common ground that this line of cases shares with other due-process jurisprudence. The Supreme Court has explained that the ultimate purpose of its *Brady* doctrine is to satisfy the due-process mandate "that a miscarriage of justice does not occur,"[211] and that *Brady* violations are unfair "not just because they involve prosecutorial misconduct, but more importantly because they involve a corruption of the truth-seeking function of the trial process."[212] These same constitutional values inform the actual-innocence cases described below, and are also relevant to a defendant's due-process entitlement to content covered by the SCA.

2. Wardius *and Reciprocity Requirements*

Brady jurisprudence is a product of prosecutors' heightened access to investigative tools relative to criminal defendants. Even if *Brady* cannot force the prosecution to deploy these tools to seek out information on behalf of the defense, powers that are reserved solely for the prosecution and inaccessible to the defense may create constitutional issues leading to alternative remedies.

The asymmetry created by the use-immunity statute discussed above offers one example. 18 U.S.C. §§ 6002-6003 allow prosecutors to compel witnesses who may have otherwise invoked their Fifth Amendment right against self-incrimination to testify, with the guarantee that their testimony will not be used against them. Criminal defendants cannot offer an equivalent guarantee. The majority of courts have found that grants of use immunity are a uniquely prosecutorial function and that therefore the evidence prosecutors can obtain through the statute is beyond the reach of criminal defendants.[213] Similar arguments in the context of the SCA may fare equally badly for criminal defendants.

Nonetheless, the Third Circuit has fashioned a remedy to level the playing field without granting use immunity to a criminal defense witness: "If the Government refuses to immunize the witness in violation of the defendant's due-process right, the trial court can dismiss the charges against the defendant."[214]

---

211. United States v. Bagley, 473 U.S. 667, 675 (1985).

212. United States v. Agurs, 427 U.S. 97, 104 (1976).

213. *See, e.g.*, United States v. Quinn, 728 F.3d 243, 247 (3d Cir. 2013) (en banc) (joining every other federal court of appeals in rejecting the "theory of judicial power" that would "permit[] a trial court to immunize a defense witness"); United States v. Capozzi, 883 F.2d 608, 613 n.7 (8th Cir. 1989) ("It is settled law that a court is without authority to immunize a witness pursuant to the federal use immunity statute." (citing Pillsbury Co. v. Conboy, 459 U.S. 248, 261 (1983))).

214. *Quinn*, 728 F.3d at 259-60.

The remedy of dismissing the charges (or vacating and allowing a new trial only if the prosecutor *does* grant immunity to the defendant's witness) is appropriate as a response to prosecutorial misconduct. Under this theory, a government's refusal to grant immunity can rise to the level of prosecutorial misconduct if the refusal to grant immunity is "solely to gain a tactical advantage against the accused," thus justifying the court's intervention.[215]

This approach provides a release valve for the due-process issues that can arise when the prosecution has a means of accessing evidence that is entirely unavailable to the defendant. Courts could adopt a similar protection in the case of the SCA. If prosecutors decline to seek covered content in a scenario where "the Government had no strong reason to keep exculpatory testimony from trial,"[216] then the prosecution may not be under any obligation to seek out that information. However, the court could instead protect the defendant's due-process rights by vacating a conviction and either allowing a new trial on the condition that the prosecution provide that evidence, and if not, dismissing the charges. This dismissal remedy has been implemented in other scenarios where the prosecution refuses to provide access to evidence that they alone have access to, such as information about the identity and communications of informers.[217]

Such a strategy would be consistent with the Supreme Court's jurisprudence on reciprocal discovery in other situations. In *Wardius v. Oregon*,[218] the Supreme Court struck down an Oregon discovery statute that required criminal defendants to provide advance notice of their alibi witnesses to the state without requiring the state to provide comparable pretrial discovery. In so holding, the Supreme Court concluded that "[a]lthough the Due Process Clause has little to say regarding the amount of discovery which the parties must be afforded, it does speak to the balance of forces between the accused and his accuser."[219] The Court referenced its watershed decisions in *Washington v. Texas*[220] and *Gideon v. Wainwright*[221] to ground its skepticism of rules that "provide nonreciprocal benefits to the State when the lack of reciprocity interferes with the defendant's ability to

215. *Id.* at 259.

216. *Id.*

217. *See* Roviaro v. United States, 353 U.S. 53, 60-61 (1957) ("Where the disclosure of an informer's identity, or of the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause . . . the trial court may require disclosure and, if the Government withholds the information, dismiss the action.").

218. 412 U.S. 470 (1973).

219. *Id.* at 474 (internal citation omitted).

220. 388 U.S. 14 (1967).

221. 372 U.S. 335 (1963).

secure a fair trial."[222] *Wardius* stands for the proposition that "in the absence of a strong showing of state interests to the contrary, discovery must be a two-way street."[223] As Colin Miller has observed, "[c]ourts across the country have since applied *Wardius* to require reciprocal discovery in cases ranging from expert witness disclosures to character witness disclosures."[224] Indeed, *Wardius* has been interpreted to apply to "any procedure denying reciprocal discovery rights . . . whether expressly pursuant to a statute or judicially created."[225]

Although *Wardius* has not been overturned, it is not invoked to enforce reciprocal discovery rights in other contexts with significant frequency. Criminal defendants and their advocates should push back against the turn away from *Wardius*, which remains good law. The Supreme Court has opened few doors to due-process rights of discovery outside of the *Brady* context,[226] so it is advantageous for advocates to seize and seek to expand the openings that do exist. The holding in *Wardius* is limited. It does not provide an absolute right to any particular type of discovery, but instead insists on some level of parity between the accused and their accuser. The downside of this approach is that it is contingent; where the prosecution does not have access to a particular form of evidence, *Wardius* alone will not grant it. But conversely, the advantage to this approach is that it is adaptable. Given that the holding in *Wardius* is relative—always considered with reference to discovery rights afforded to the prosecution—it is uniquely well-suited to keep up with technological advances, which will frequently benefit the prosecution before even becoming available to the defense. As described in the next Section focusing on actual innocence, due-process rights are frequently difficult to establish in the context of new technology. Due-process analysis relies heavily on history and tradition,[227] and it can be difficult to locate emerging technologies within case law that developed at a time they did not exist. Yet a due-process right that is frozen in time will eventually come to lose its meaning. *Wardius*'s reciprocity requirement provides a framework to bridge the gap between well-established due-process principles and new developments in criminal evidence, and should be revitalized to serve that purpose.

In practice, the SCA denies reciprocal discovery rights in violation of *Wardius*. By creating a significant privacy asymmetry, the SCA has disrupted the

---

222. *Wardius*, 412 U.S. at 474 n.6.

223. *Id.* at 475.

224. Colin Miller, *Reciprocal Immunity*, 93 IND. L.J. SUPPLEMENT 1, 7 (2018) (citing Grey v. State, 178 P.3d 154, 159-61 (Nev. 2008); State v. Pond, 193 P.3d 368, 380-82 (Haw. 2008)).

225. United States *ex rel*. Veal v. DeRobertis, 693 F.2d 642, 647 (7th Cir. 1982).

226. *See, e.g.*, Weatherford v. Bursey, 429 U.S. 545, 559 (1977) ("There is no general constitutional right to discovery in a criminal case . . . .").

227. *See infra* notes 255-258 and accompanying text.

balance of forces between the accused and the accuser. The Supreme Court has held that "it is rarely justifiable for the prosecution to have exclusive access to a storehouse of relevant fact."[228] Under the SCA as it currently stands, the prosecution could obtain and introduce evidence of threatening messages a criminal defendant sent to a victim of an alleged crime. But if that same criminal defendant had knowledge of threatening messages a third party sent to the victim, the SCA would bar the defendant from accessing them, preventing the introduction of this potentially exculpatory evidence at trial.[229] There is no strong governmental interest in denying criminal defendants access to covered content under the SCA. Thus, interpreting the statute to allow government discovery while denying the defense access to the same information violates due process.

To the extent that the Supreme Court has sanctioned asymmetries in discovery rights, the imbalances have benefitted the *defendant*, not the prosecution. As Mark J. Mahoney points out, *Washington v. Texas*[230] and *Chambers v. Mississippi*[231] stand for the proposition that "the accused is entitled to more than parity with the state in the presenting of the defense."[232] The reason for this is the different stakes at issue for the defendant and the prosecution—namely, the defendant's potential loss of liberty. Indeed, the Court has stated that, "[t]he asymmetrical nature of the Constitution's criminal-trial guarantees is not an anomaly, but the intentional conferring of privileges designed to prevent criminal conviction of the innocent. The State is at no risk of that."[233]

This distinction means that, in addition to the free-standing right to evidence grounded in due process and the Sixth Amendment, the fact that prosecutors can access content covered by the SCA bolsters a criminal defendant's right of access. It is worth noting that eliminating this imbalance by revoking the prosecution's access to the contents of electronic communications might address the asymmetry element of the due-process concerns. Doing so, however, is not responsive to a criminal defendant's standalone rights to access exculpatory

228. Dennis v. United States, 384 U.S. 855, 873 (1966).

229. This is not the case if the messages in question were in the possession of the prosecution, in which case they would likely be subject to *Brady* disclosures. However, the prosecution may not have an incentive to pursue and obtain messages from third parties who have not been charged.

230. 388 U.S. 14 (1967).

231. 410 U.S. 284 (1973).

232. *See* Mark J. Mahoney, *The Right to Present a Defens*e, N.Y. ST. ASS'N CRIM. DEF. LAWS. 174 (Dec. 2, 2016), https://www.harringtonmahoney.com/content/Publications/Mahoney%20-%20Right%20to%20Present%20a%20Defense%202017.pdf [https://perma.cc/L5T9-M58A].

233. Giles v. California, 554 U.S. 353, 376 n.7 (2008); *see also* Mahoney, *supra* note 232, at 170 (analyzing this quotation from *Giles*).

evidence and present a defense as described below. Thus, taking those rights into account, the constitutional-asymmetry argument requires granting the defense access to evidence—not leveling the playing field by reducing the prosecution's access. If the defendant cannot gain access, then courts must fashion a remedy like the one the Third Circuit adopted in *Quinn*: vacating the conviction and dismissing the charges in the event that the defendant cannot access the evidence at issue.[234]

3. Actual Innocence

The due-process interest in accuracy underlying *Brady* and *Wardius* also motivates a separate line of cases offering protection to individuals with proof of actual innocence. This line of cases is rooted in a defendant's liberty interest in demonstrating actual innocence and thus protects a core tenant of due-process doctrine. The Supreme Court has clearly articulated that the "ultimate objective" of the American criminal justice system is that "the guilty be convicted and the innocent go free."[235] Much of the Supreme Court's criminal-procedure jurisprudence is therefore focused on accuracy in convictions.[236] Individuals who are actually innocent have a strong due-process liberty interest that is protected by constitutional criminal procedure, including access to evidence.

Both substantive and procedural due process apply to claims of actual innocence. Substantive due process protects individuals from governmental action that "shocks the conscience"[237] or interferes with rights that are "implicit in the concept of ordered liberty."[238] Criminal punishment of individuals who are actually innocent satisfies both of these standards. Procedural due process, on the other hand, requires that even if a deprivation enacted by the government is con-

---

234. *See* United States v. Quinn, 728 F.3d 243, 259-60 (3d Cir. 2013).

235. Herring v. New York, 422 U.S. 853, 862 (1975).

236. *See* Brandon L. Garrett, *DNA and Due Process*, 78 FORDHAM L. REV. 2919, 2945 (2010) (explaining that "rules regulating eyewitness identifications, confessions, defense access to expert assistance, and defense access to exculpatory evidence" are all related to "concerns regarding accuracy").

237. Rochin v. California, 342 U.S. 165, 172 (1952).

238. Palko v. Connecticut, 302 U.S. 319, 324-25 (1937). Although *Palko* has been overruled, the Supreme Court and lower courts continue to rely on the proposition that due process "requires state criminal trials to provide defendants with protections 'implicit in the concept of ordered liberty.'" Danforth v. Minnesota, 552 U.S. 264, 269-270 (2008) (quoting *Palko*, 302 U.S. at 325); *see also* Washington v. Glucksberg, 521 U.S. 702, 720-21 (1997) (citing *Palko*, 302 U.S. at 325); McKinney v. Pate, 20 F.3d 1550, 1556 (11th Cir. 1994) (same); Heike v. Guevara, 519 F. App'x 911, 923 (6th Cir. 2013) (same).

sistent with the substantive requirements outlined above, it must be implemented in a fair manner. This is the root of criminal defendants' "right to a fair opportunity to defend against the State's accusations."[239]

While the actual-innocence doctrine was largely developed in capital cases, it applies to criminal prosecutions more broadly. As the Supreme Court explained in *Herrera v. Collins*: "It would be a rather strange jurisprudence . . . which held that under our Constitution [the actually innocent] could not be executed, but that he could spend the rest of his life in prison."[240] It is important to note that "actual innocence" not only encompasses instances where the defendant did not do what he was charged with, but can also include cases where the defendant did perform the conduct at issue but has a complete defense to it.[241] This is relevant because while the SCA's bar on access to evidence can be implicated in capital cases,[242] many instances of criminal defendants seeking evidence covered by the SCA occur in noncapital cases in which the defendants are claiming self-defense.[243] The contents of electronic communications could also be used to support what is more conventionally thought of as "factual innocence," a subset of actual innocence. For example, social-media alibi evidence that establishes the defendant was not at the scene of the crime or that identifies the real perpetrator of the conduct at issue would contribute to a claim of factual innocence.

It is important to note that much of the actual-innocence doctrine was developed in the postconviction setting, where due-process rights are more limited.[244] The liberty interest of defendants seeking exculpatory evidence at trial

239. Chambers v. Mississippi, 410 U.S. 284, 294 (1973).

240. Herrera v. Collins, 506 U.S. 390, 405 (1993).

241. A defendant with a complete affirmative defense could qualify as "actually innocent" because the state would not be able to prove all of the requisite elements of the crime. For example, in the habeas context, the Ninth Circuit has held that a claim of "justification pursuant to self-defense . . . corresponds with *Schlup*'s actual innocence requirement" because under state law "justification was an affirmative defense rendering the [defendant's] conduct noncriminal." Jaramillo v. Stewart, 340 F.3d 877, 883 (9th Cir. 2003) (citing Schlup v. Delo, 513 U.S. 298 (1995)). Relatedly, the Seventh Circuit has rejected the argument that "actual innocence" requires a habeas petitioner to show that he "didn't kill his victim." Britz v. Cowan, 192 F.3d 1101, 1103 (7th Cir. 1999).

242. *See* Petition for Writ of Certiorari at 3-5, Colone v. Superior Ct., 142 S. Ct. 77 (2021) (No. 20-1474); Colone v. Superior Ct. (*GitHub*), No. S265307 (Cal. Jan. 13, 2021) (judgment and order denying petition for review).

243. *See, e.g.*, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 387 (Cal. 2020); Facebook, Inc. v. Pepe, 241 A.3d 248, 251-52 (D.C. 2020).

244. *See, e.g.*, Dist. Att'y's Off. for the Third Jud. Dist. v. Osborne, 557 U.S. 52, 69 (2009) (noting that when seeking postconviction relief, the defendant's "right to due process is not parallel to a trial right").

has been traditionally recognized as stronger, which lends weight to defendants who seek to assert their due-process rights to access evidence under the SCA at trial.

To determine whether a particular practice—in this case, the denial of evidence pursuant to the SCA—violates due process, a court will consider whether the criminal procedures at issue "offend[] some principle of justice so rooted in the traditions and conscience of our people as to be ranked as fundamental."[245] This is the test the Supreme Court established in *Medina v. California*[246] when it declined to impose the more inclusive due-process test developed in *Mathews v. Eldridge*.[247] While the applicability of the *Medina* test compared to the traditional *Eldridge* due-process balancing test is not entirely doctrinally clear,[248] this Note takes on the higher burden of the *Medina* test to suggest that barring defendants access to exculpatory evidence pursuant to the SCA violates either due-process standard.

The ability of a defendant to access exculpatory evidence at trial is a fundamental principle of justice, consistent with the body of due-process case law outlined above. If a defendant is denied the opportunity to access exculpatory evidence only because of the SCA, that denial violates the fundamental principles of justice implicated in actual-innocence claims. The well-established due-process emphasis on accuracy and fundamental fairness suggests that a statutory denial of exculpatory evidence violates due process. To hold otherwise would elevate social-media evidence into a protected category entirely out of line with other forms of evidence implicating privacy concerns. Indeed, as counsel for a criminal defendant seeking access to content under the SCA asked:

---

245. Medina v. California, 505 U.S. 437, 446 (1992) (quoting Patterson v. New York, 432 U.S. 197, 202 (1977)).

246. *See id.* at 442-46.

247. 424 U.S. 319 (1976).

248. *See* Daniel S. McConkie, *Structuring Pre-Plea Discovery*, 107 J. CRIM. L. & CRIMINOLOGY 1, 42 (2017) ("The Court has never definitively decided whether it will apply the deferential *Medina* test or the *Eldridge* (*Ake*) test to criminal due process cases." (citing Kaley v. United States, 571 U.S. 320, 334 (2014))); *see also* United States v. Ruiz, 536 U.S. 622, 631 (2002) (applying the due-process balancing test in the criminal context a decade after *Medina*); E. THOMAS SULLIVAN & TONI M. MASSARO, THE ARC OF DUE PROCESS IN AMERICAN CONSTITUTIONAL LAW 97 (2013) ("In *Medina*, the same decision in which the Court rejected [the] *Eldridge* balancing approach, the concurring and dissenting opinions noted that the majority used an analysis that was strikingly similar to the flexible analysis employed in *Eldridge*."); Jason Kreag, *Letting Innocence Suffer: The Need for Defense Access to the Law Enforcement DNA Database*, 36 CARDOZO L. REV. 805, 857-58 (2015) (arguing that the "break" from due-process balancing "was far from clean").

> How is it that defense counsel may readily and righteously obtain confidential medical, cell phone, and psychiatric records of a complaining witness, while their social media records are entirely unobtainable under the law? This is not the system of justice envisioned by Congress when they enacted the Stored Communications Act, and it is not the system of justice this Court should enforce.[249]

Actual-innocence cases making arguments for access to other forms of evidence provide a strong foundation for criminal defendants seeking to assert a due-process right to exculpatory evidence under the SCA.[250]

Academics and litigators have made comparable arguments drawing on *Brady*, *Wardius*, and actual-innocence jurisprudence in the context of access to postconviction DNA evidence. In the same way that the *Brady* doctrine is not directly applicable to SCA evidence, it similarly does not directly cover this form of DNA evidence, because *Brady* rights are not established in a postconviction setting.[251] However, advocates have suggested that the rights that underlie *Brady* (and implicitly also *Wardius*) in combination with the Supreme Court's actual-innocence jurisprudence establish a due-process right to postconviction defense-initiated DNA testing and database searches.[252]

In the context of access to postconviction DNA, Jason Kreag details the following question under *Medina*:

> Does it violate traditional and fundamental principles of justice for the state to create and use a law enforcement tool that is so powerful that it can categorically prove innocence and confirm guilt in a certain subset of criminal cases, yet at the same time deny access to this tool to defendants in the same subset of cases who seek to prove their innocence?[253]

---

249. Real Party in Interest Touchstone's Response to San Diego District Attorney Intervenor Brief at 11, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203).

250. For a summary of federal and state constitutional case law on actual innocence, see John M. Leventhal, *A Survey of Federal and State Courts' Approaches to a Constitutional Right of Actual Innocence: Is There a Need for a State Constitutional Right in New York in the Aftermath of CPL § 440.10(G-1)?*, 76 ALB. L. REV. 1453 (2013).

251. *See* Dist. Att'y's Off. for the Third Jud. Dist. v. Osborne, 557 U.S. 52, 69 (2009).

252. *See* Garrett, *supra* note 236, at 2957-60; Kreag, *supra* note 248, at 858-60. These articles both contend with *Osborne*, 557 U.S. 52, and ultimately argue that the case does not preclude a due-process right to postconviction DNA evidence in certain circumstances. *See* Garrett, *supra* note 236, at 2957-60; Kreag, *supra* note 248, at 840-44.

253. Kreag, *supra* note 248, at 857.

Kreag answers the question in the affirmative.[254] One might ask a similar question about access to social-media evidence; the Court's due-process jurisprudence on accuracy and the ways in which this form of asymmetry violates fundamental fairness suggest that the answer is yes in that setting as well.

Modern due-process arguments like the one outlined above—particularly under the higher standard of *Medina*—can often be hindered by the Court's privileging of historical practices.[255] In the case of emerging technologies, there is often no historical practice to ground the due-process analysis. However, the lack of analogous historical practices does not eliminate a defendant's right to access evidence. Instead, it counsels in favor of adapting jurisprudence to expand access to newly available sources of information. The advent of the immense wealth of data created by emails, social-media records, and other new technologies offers a pathway to vindicate criminal defendants' rights in ways that were previously not possible. But that previous impossibility does not mean that those rights are not constitutionally protected today. In her concurrence in *Medina*, Justice O'Connor recognized that the Supreme Court's due-process jurisprudence has "required States to institute procedures that were neither required at common law nor explicitly commanded by the text of the Constitution."[256] This is consistent with longstanding interpretations of due process, including Justice Frankfurter's assertion that "[d]ue process is perhaps the most majestic concept in our whole constitutional system. While it contains the garnered wisdom of the past in assuring fundamental justice, it is also a living principle not confined to past instances."[257] After all, due process "is, perhaps, the least frozen concept of our law—the least confined to history and the most absorptive of powerful social standards of a progressive society."[258]

---

254. *See id.* at 857-58.

255. *See* Medina v. California, 505 U.S. 437, 446 (1992) ("Historical practice is probative of whether a procedural rule can be characterized as fundamental."); *see also* Kathryn E. Miller, *The Attorneys Are Bound and the Witnesses Are Gagged: State Limits on Post-Conviction Investigation in Criminal Cases*, 106 CALIF. L. REV. 135, 185 (2018) (advocating in favor of the *Eldridge* test to assess practices "that limit a criminal defendant's ability to seek redress for the violation of his federal constitutional rights because of its emphasis on fairness," and noting that "[t]he problem with the *Patterson* test [taken up in *Medina*] is that it privileges historical practice at the expense of procedural fairness").

256. *Medina*, 505 U.S. at 454 (O'Connor, J., concurring).

257. Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 174 (1951) (Frankfurter, J., concurring).

258. Griffin v. Illinois, 351 U.S. 12, 20-21 (1956) (Frankfurter, J., concurring in the judgment).

Indeed, the fact that "digital data . . . does not fit neatly under existing precedents" has not stopped the Supreme Court from extending constitutional protections to it in the past.[259] While defendants have not previously had the opportunity to access the contents of communications, this fact cannot be used to deprive them of a right to such access now that technology has advanced to make access possible.

B. Sixth Amendment Rights

Sixth Amendment protections overlap with and reinforce the due-process rights afforded to criminal defendants. Specifically, the Sixth Amendment guarantees that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him" and "to have compulsory process for obtaining witnesses in his favor."[260] The SCA's bar on accessing the content of communications may therefore also implicate a criminal defendant's Sixth Amendment rights.

Criminal defendants can assert their Sixth Amendment rights at trial to support their arguments of constitutional entitlement to evidence. The denial of evidence pursuant to the SCA may also serve as the basis for an appeal. Depending on the details of their arguments on appeal, the defendant may need to show (as they would in a *Brady* argument) that access to the evidence would have resulted in a different outcome. As described above, this inquiry depends on what specific electronic communications the defendant is seeking.[261] But electronic communications that would have functioned as a compelling independent corroboration of a failed alibi witness or the primary evidence of threats central to a self-defense claim could certainly rise to this level.

This Section details three specific Sixth Amendment rights that are relevant to a criminal defendant's ability to access information under the SCA. First, the right to confrontation and the associated right to cross-examination may require the production of evidence covered under the SCA to effectively cross-examine witnesses. Second, the Compulsory Process Clause guarantees criminal defendants a meaningful opportunity to present a defense, which may similarly hinge on the ability to present relevant evidence. Third, the right to effective assistance

259. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (holding that a warrantless acquisition of cell-site records violated the Fourth Amendment right against unreasonable searches and seizures).

260. U.S. CONST. amend. VI.

261. See *supra* Section IV.A.1 on the need to show that the evidence prosecutors withheld would have resulted in a different outcome to establish a *Brady* violation.

of counsel hinges on counsel's ability to investigate and procure evidence, which also implicates the SCA's prohibition on access.

1. Right to Confrontation and Cross-Examination

The Confrontation Clause of the Sixth Amendment provides that "in all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him."[262] In *Pennsylvania v. Ritchie*, which expounds upon both the Confrontation Clause and its corollary Compulsory Process Clause, the Supreme Court explained that "[t]he Confrontation Clause provides two types of protections for a criminal defendant: the right physically to face those who testify against him, and the right to conduct cross-examination."[263] Records covered by the SCA may be crucial to effectively cross-examine witnesses. For example, the contents of electronic communications could be necessary to impeach a witness, to show bias, to demonstrate prejudice, or to attack a witness's credibility. A defendant's ability to take these steps is protected by the Confrontation Clause.[264] The production of electronic communications might therefore be a necessary prerequisite for some criminal defendants to vindicate their constitutional right to confrontation and cross-examination.

The Supreme Court has held that without the opportunity "to expose to the jury the facts from which jurors, as the sole triers of fact and credibility, could appropriately draw inferences relating to the reliability of the witness," defendants are "denied the right of effective cross-examination which 'would be constitutional error of the first magnitude and no amount of showing of want of prejudice would cure it.'"[265] If a defendant cannot secure important information from witnesses' electronic communications, then the same violation would occur.

Given the circuit split as to whether the Confrontation Clause attaches at trial,[266] these arguments may offer limited help to criminal defendants whose cases do not advance to trial. Nonetheless, it may prove helpful for criminal de-

262. U.S. CONST. amend. VI.

263. 480 U.S. 39, 51 (1987) (plurality opinion) (citing Delaware v. Fensterer, 474 U.S. 15, 18-19 (1985)).

264. Davis v. Alaska, 415 U.S. 308, 315-317 (1974).

265. *Id.* at 318 (quoting Brookhart v. Janis, 384 U.S. 1, 3 (1966)).

266. *See* Christine Holst, *The Confrontation Clause and Pretrial Hearings: A Due Process Solution*, 2010 U. ILL. L. REV. 1599, 1600.

fendants who do proceed to trial, and there are strong arguments for the Confrontation Clause's application at the pretrial stage.[267] But even under current precedent holding that the Confrontation Clause is not a "constitutionally compelled rule of pretrial discovery,"[268] the Confrontation Clause could be successfully invoked to secure access to evidence at trial.

The Eighth Circuit has applied this principle in the context of privileged medical records in an approach that could serve as a model for how the Confrontation Clause could be leveraged to help defendants secure contents of communications covered by the SCA. In *United States v. Arias*, a defendant challenged his conviction on the grounds that the trial court violated his Confrontation Clause rights by allowing a witness to testify to her mental health while denying the defendant access to the witness's mental-health records.[269] Although the court found no error in the original pretrial ruling denying access to the records, it also held that once the topic was broached at trial, "if the records revealed that there was no diagnosis, then Arias was denied the opportunity to cross-examine on an issue which would have directly related to [the witness's] credibility in a case that rested entirely on conflicting testimony."[270] This case also demonstrates how the Confrontation Clause could extend a criminal defendant's access to evidence beyond the scope covered by the discussion of *Brady* in Section IV.A.1. In *Arias*, the court noted that "[a]t no point during the relevant proceedings was the government in possession of the requested treatment records."[271] Further, it demonstrates that the Confrontation Clause can serve to vindicate a criminal defendant's rights even when the evidence at issue is protected by some other bar against disclosure: in *Arias*, the records were protected by psychotherapist-patient privilege.[272] The Court circumvented the privilege concerns by ordering an in camera review of records,[273] which could also serve as a workaround in the SCA context.

2. *Right to Compulsory Process*

While the Confrontation Clause pertains to a defensive right to protect against the testimony offered by the prosecution's witnesses, the Compulsory

267. *Id.* at 1614-16; *see also* William Ortman, *Confrontation in the Age of Plea Bargaining*, 121 COLUM. L. REV. 451 (2021).

268. *Ritchie*, 480 U.S. at 52.

269. 936 F.3d 793, 796 (8th Cir. 2019).

270. *Id.* at 799.

271. *Id.* at 795.

272. *Id.*

273. *Id.* at 800.

Process Clause offers criminal defendants an affirmative right "to have compulsory process for obtaining witnesses in [their] favor."[274] The Supreme Court has established that "[w]hether rooted directly in the Due Process Clause of the Fourteenth Amendment or in the Compulsory Process or Confrontation Clauses of the Sixth Amendment, the Constitution guarantees criminal defendants 'a meaningful opportunity to present a complete defense.'"[275] The Court explained in *United States v. Nixon*:

> The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense.[276]

Given the increasing importance of digital evidence, the holding in *Nixon* suggests that criminal defendants' compulsory-process rights support their ability to access digital evidence. These rights are directly relevant to the type of evidence covered by the SCA. The right to present a defense includes "[t]he right to offer the testimony of witnesses, and to compel their attendance, if necessary."[277] Generally speaking, it comprises "the right to present the defendant's version of the facts as well as the prosecution's to the jury so it may decide where the truth lies."[278] The contents of communications may in some cases be central to the defendant's ability to present their own "version of the facts."

Courts have enforced compulsory-process rights even when they conflict with statutory bars on disclosure such as the bar featured in the SCA.[279] Privacy interests of the sort implicated by the SCA are insufficient to override a criminal

---

274. U.S. CONST. amend. VI.

275. Holmes v. South Carolina, 547 U.S. 319, 324 (2006) (quoting Crane v. Kentucky, 476 U.S. 683, 690 (1986)).

276. United States v. Nixon, 418 U.S. 683, 709 (1974).

277. Washington v. Texas, 388 U.S. 14, 19 (1967).

278. *Id.*

279. *See, e.g.*, Pennsylvania v. Ritchie, 480 U.S. 39, 57 (1987) (stating that a Pennsylvania statute did not provide an agency with an absolute shield from disclosure); Davis v. Alaska, 415 U.S. 308, 319 (1974) (holding that the rights of a defendant to cross-examine a witness outweighed the state's interest in protecting the identities of juvenile offenders).

defendant's compulsory-process rights—indeed, in a case where there is an existing pathway for disclosure (as there is in the SCA through the law-enforcement exception, which precludes the statute from enforcing an unequivocal privacy protection), privacy interests are even more likely to succumb to compulsory process interests.[280]

In order to vindicate a criminal defendant's right to compulsory process, the Supreme Court has in some cases mandated the assistance of the prosecution, which may have greater powers at its disposal than the defense. For example, the Supreme Court has held that while the Court has "had little occasion to discuss the contours of the Compulsory Process Clause . . . . [o]ur cases establish, at a minimum, that criminal defendants have the right to the government's assistance in compelling the attendance of favorable witnesses at trial."[281]

Much as the Compulsory Process Clause has been read to require the government's cooperation in procuring witnesses to ensure a defendant's opportunity to present a defense, it could be read to require the government's cooperation in procuring evidence. While the language of the Compulsory Process Clause refers to witnesses, settled jurisprudence indicates that it comprises the right to present a defense more broadly and includes documents.[282] The prosecution's obligation to use its unique powers and authority to procure defense witnesses is comparable to an obligation to secure evidence that is exclusively within its own power to obtain (such as the contents of electronic communications covered by the SCA) when that evidence implicates the Compulsory Process Clause and is unavailable to the defense independently. The Compulsory Process Clause could therefore serve to either provide a pathway for defendants to access—an imperfect solution, for the reasons discussed in Section III.A.2—or, if the evidence cannot be procured, a justification for a court to hold the SCA unconstitutional as applied.

Notably, the Court's compulsory-process jurisprudence shows a willingness to adapt to changing circumstances, as opposed to allowing the Compulsory Process Clause to be governed by "the dead hand of the common-law rule of 1789."[283] In *Washington v. Texas*, the Supreme Court identified a violation of the Compulsory Process Clause when a defendant was disqualified from presenting

---

280. *Ritchie*, 480 U.S. at 57-58, 61.

281. *Id.* at 55-56.

282. *See* Mahoney, *supra* note 232, at 36-37 ("Each defense subpoena implicates 'the right to present a defense' acknowledged by the Supreme Court in *Washington v. Texas*, 388 U.S. 14 (1967). Some have argued that the literal terms of the Compulsory Process Clause—referring to 'witnesses' and nothing else—does not cover *documents* or other objects. This argument was dispelled at the very outset, in the *Burr* case, where Burr was allowed to subpoena the letters from President Jefferson and the Attorney General, despite this precise argument.").

283. *Washington*, 388 U.S. at 22 (quoting Rosen v. United States, 245 U.S. 467, 471 (1918)).

testimony from his accomplice, despite the fact that these disqualifications were widespread at the time that the Compulsory Process Clause was ratified.[284] This willingness to diverge from historical practices makes the Compulsory Process Clause particularly helpful in cases involving defendants' rights as they relate to emerging technologies, which are often hamstrung by the lack of historical precedent. Since Compulsory Process Clause jurisprudence has directly *conflicted* with historical precedent in favor of the modern-day rights of criminal defendants, the fact that there is no historical precedent for access to electronic communications should not prevent such a right from being recognized today. Further, the Compulsory Process Clause implicates rights that attach before trial,[285] another helpful feature given the minority of cases that proceed to trial.

3. Right to Effective Assistance of Counsel

The constitutional obligations described above are deeply intertwined with a defendant's right to counsel. Importantly, the right to counsel specifically guarantees *effective* assistance.[286] Without access to crucial evidence, counsel cannot provide meaningful assistance. Defense counsel has a duty to investigate and pursue all potentially exonerating evidence. As the Supreme Court explained in *Strickland v. Washington*, "a fair trial is one in which evidence subject to adversarial testing is presented to an impartial tribunal for resolution of issues defined in advance of the proceeding."[287] Evidence is central to effective assistance of counsel, as *Strickland* further warns that "counsel has a duty to make reasonable investigations or to make a reasonable decision that makes particular investigations unnecessary."[288] Scholars have argued more broadly that "pre-plea discov-

---

284. *Id.* at 16, 19-22; *see also* Jean Montoya, *A Theory of Compulsory Process Clause Discovery Rights*, 70 IND. L.J. 845, 846 (1995) (describing how in *Washington v. Texas*, the Supreme Court "found a violation of the Compulsory Process Clause when the defendant, charged with a shooting-related homicide, was allowed to subpoena but not present the testimony of the alleged trigger-puller. The Court reached this conclusion despite the fact that laws restricting a defendant's use of accomplice testimony were prevalent at the time the Bill of Rights was ratified." (footnotes omitted)).

285. *See* Peter Westen, *Confrontation and Compulsory Process: A Unified Theory of Evidence for Criminal Cases*, 91 HARV. L. REV. 567 (1978); Montoya, *supra* note 284, at 852-55, 864-71; Mahoney, *supra* note 232, at 14 ("[T]he compulsory process clause applies prior to trial and even prior to indictment, to the efforts of the defendant to obtain impeaching evidence, and independent witnesses.").

286. "It has long been recognized that the right to counsel is the right to the effective assistance of counsel." McMann v. Richardson, 397 U.S. 759, 771 n.14 (1970).

287. 466 U.S. 668, 685 (1984).

288. *Id.* at 691.

ery is necessary to effectuate defense counsel's Sixth Amendment duty to investigate and provide competent advice."[289] In other words, a criminal defense attorney's duty to investigate implies the power to investigate.[290]

Criminal defendants can be deprived of their right to effective assistance of counsel either through the actions of their attorney (i.e., "failure to render 'adequate legal assistance'"), but also through the actions of the government if the government imposes undue restrictions on defense counsel.[291] Specifically, the "[g]overnment violates the right to effective assistance when it interferes in certain ways with the ability of counsel to make independent decisions about how to conduct the defense."[292] Denying access to potentially exculpatory evidence rises to the level of preventing counsel from making independent decisions about how to conduct the defense.

This similarly applies to the defense's right to access exculpatory evidence covered by the SCA. Given that the right to counsel attaches at an early stage of criminal proceedings,[293] which is not true of all rights that extend to criminal defendants,[294] this argument may be helpful at a stage when other constitutional arguments would not succeed. On the other hand, much like *Brady*, a finding of ineffective assistance of counsel alone will not guarantee a remedy. A criminal defendant must also show prejudice to successfully invoke their right to effective assistance of counsel. That is, in addition to demonstrating ineffective assistance of counsel, the criminal defendant must demonstrate "that counsel's errors were so serious as to deprive the defendant of a fair trial, a trial whose result is reliable."[295] Although this requirement can be difficult to prove, the deprivation of exculpatory evidence from counsel could rise to that level in particularly egregious cases. It may be easier to show prejudice where the defendant is generally

289. McConkie, *supra* note 248, at 37 (citing Russell D. Covey, *Plea-Bargaining Law After* Lafler *and* Frye, 51 DUQ. L. REV. 595, 611-12 (2013)); *see also* John G. Douglass, *Fatal Attraction? The Uneasy Courtship of* Brady *and Plea Bargaining*, 50 EMORY L.J. 437, 441 n.17 (2001) (referencing scholars who argue in favor of pre-plea disclosure requirements).

290. Meyn, *supra* note 58, at 1091 n.1 (citing Williams v. Taylor, 529 U.S. 362, 396 (2000)).

291. *Strickland*, 466 U.S. at 686 (quoting Cuyler v. Sullivan, 446 U.S. 335, 344 (1980)).

292. *Id. See generally* Jenny Roberts, *Too Little, Too Late: Ineffective Assistance of Counsel, the Duty to Investigate, and Pretrial Discovery in Criminal Cases*, 31 FORDHAM URB. L.J. 1097 (2004) (arguing that there should be a Sixth Amendment analysis of restrictive discovery rules).

293. "[A] criminal defendant's initial appearance before a judicial officer, where he learns the charge against him and his liberty is subject to restriction, marks the start of adversary judicial proceedings that trigger attachment of the Sixth Amendment right to counsel." Rothgery v. Gillespie Cnty., 554 U.S. 191, 213 (2008).

294. For example, many courts have interpreted Supreme Court jurisprudence to reach the conclusion that the Confrontation Clause does not attach until trial, or alternatively, that it provides weaker protections pretrial. Holst, *supra* note 266, at 1616 nn.142-43 (collecting cases).

295. *Strickland*, 466 U.S. at 687.

already aware of what the contents of the communications in question are likely to reveal.

CONCLUSION

Despite the fact that the forms of communication that the SCA governs in the modern era did not even exist at the time it was drafted, the text of the SCA has remained unchanged from the time of its enactment. The statute's outdated understandings of technology and failure to adapt to the realities of modern criminal evidence have cost many criminal defendants dearly. Unable to rely on communications covered by the SCA, criminal defendants whose case requires evidence that happens to come in the form of electronic communications have faced lengthy prison sentences[296] and, in at least one case, a death sentence.[297]

This Note offers a comprehensive overview of strategies criminal defendants can pursue to avoid these outcomes until the much-needed statutory amendments for which activists and academics have long advocated are passed.[298] This Note's novel analysis of existing SCA case law in the criminal context provides for a comprehensive overview of the pathways to accessing evidence that are available to criminal defendants, and also sheds light on which strategies are likely to be successful. Finally, this Note takes one step further than existing scholarly literature pointing to the problems with the SCA's applications to criminal defendants by making the argument that the statute is unconstitutional as applied in cases where it blocks access to exculpatory evidence.

While this Note has laid out each of these constitutional arguments individually, the court need not necessarily parse them in this way—the constitutional arguments interact with and strengthen one another, jointly falling within the

---

296. *See, e.g.*, United States v. Wenk, 319 F. Supp. 3d 828 (E.D. Va. 2017); *see also Midlothian Businessman Sentenced to Prison for Fraud*, U.S. ATT'Y'S OFF.: E. DIST. VA. (July 11, 2018), https://www.justice.gov/usao-edva/pr/midlothian-businessman-sentenced-prison-fraud [https://perma.cc/YU3M-G34T] (noting that Timothy Scott Wenk was sentenced to twelve years in prison for fraud).

297. *See* Petition for Writ of Certiorari at 4, Colone v. Superior Ct., 142 S. Ct. 77 (2021) (No. 20-1474) ("Despite Mr. Colone's appropriate subpoena issued in San Francisco Superior Court, California courts have unanimously refused to enforce the subpoena. The lower courts held that a confidentiality provision in the Stored Communications Act (SCA), 18 U.S.C. § 2702(a), categorically bars criminal defendants from subpoenaing the contents of online communications, even where those communications otherwise implicate no privacy interest and are necessary to the litigation concerning the constitutionality of Mr. Colone's conviction and death sentence.").

298. *See, e.g.*, Kerr, *supra* note 93, at 1233-42; Sasso, *supra* note 164, at 57-62; Wexler, *supra* note 9, at 258-62; Zwillinger & Genetski, *supra* note 78, at 597-98.

due-process and Sixth Amendment protections that together comprise "the area of constitutionally guaranteed access to evidence."[299]

In addition to the overlap and symbiosis between the constitutional arguments, the constitutional and statutory interpretation strategies are also closely interconnected: Even if a court is unwilling to find the SCA unconstitutional as applied, the doctrine of constitutional avoidance may push courts towards favorable statutory readings that allow criminal defendants access to evidence under the SCA in cases where defendants raise constitutional concerns.

The SCA serves as a case study of broader concerns on inequities in criminal defendants' access to information that apply to other statutes with privacy asymmetries as well. As digital evidence becomes more important in criminal proceedings, courts, legislators, defense counsel, and criminal defendants themselves must stay alert to the ways in which outdated and imbalanced statutes infringe upon their rights—and the ways in which they can use these statutes and their constitutional rights to obtain the evidence they need despite these asymmetries.

299. United States v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982).