7-12-2023

Future-Proofing U.S. Laws for War Crimes Investigations in the Digital Era

Rebecca Hamilton

FUTURE-PROOFING U.S. LAW FOR WAR CRIMES INVESTIGATIONS IN THE DIGITAL ERA

Rebecca J. Hamilton[*]

Advances in information technology have irrevocably changed the nature of war crimes investigations. The pursuit of accountability for the most serious crimes of concern to the international community now invariably requires access to digital evidence. The global reach of platforms like Facebook, YouTube, and Twitter means that much of that digital evidence is held by U.S. social media companies, and access to it is subject to the U.S. Stored Communications Act.

This is the first Article to look at the legal landscape facing international investigators seeking access to digital evidence regarding genocide, war crimes, crimes against humanity, and aggression. It analyzes Republic of Gambia v. Facebook *(Meta), the first case to seek digital evidence from a U.S. social media company for an international proceeding on genocide. And it draws on material gleaned from background interviews with international investigators seeking digital evidence held by U.S. social media companies in relation to atrocities in Myanmar and Ukraine. This reveals two key problems facing international investigators. First, and in contrast to their counterparts in domestic criminal investigations, the Stored Communications Act provides no pathway through which international investigators can overcome the prohibition on disclosure of private digital evidence. Second, the ability of international investigators to access quasi-public digital evidence, and/or digital evidence that was public but has been removed by a social media company, is at the discretion of the*

[*] Professor of Law, American University, Washington College of Law; Visiting Fellow, Yale Law School Information Society Project (ISP). This Article has benefited immensely from feedback and engagement by Anupam Chander, MJ Durkee, Duncan Hollis, Asaf Lubin, and the students, fellows and faculty at Temple Law School Institute for Innovation, Law and Technology, the Georgetown University Law Center Technology Colloquium, the University of Georgia Law Review Symposium, and the Yale Mass Atrocities in the Digital Era project. Special thanks to Hannah Friedrich for stellar research assistance and to the phenomenal UGA Law Review editors for their thorough work. All errors are my own.

social media company. A significant risk emerging from this arrangement is that evidence disclosure decisions are not made in a consistent and principled manner, but are instead driven by the self-interest of a few U.S. corporations, creating disparate outcomes across victim groups.

The Article recommends two, non-exclusive, reforms that could be undertaken in the short term to advance principled disclosure decisions for accountability, while ensuring privacy protections and data security. It also urges U.S. social media companies to develop and publish their own interim guidelines on how they make evidence disclosure decisions, with a presumption in favor of disclosing removed public and quasi-public evidence needed for the pursuit of accountability for the international crimes of genocide, war crimes, crimes against humanity, and aggression. The Article concludes by pointing to the need for a long-term incremental process of research, reform, and review to future-proof U.S. law for war crimes accountability in the digital era.

TABLE OF CONTENTS

I. INTRODUCTION

Citizens in conflict zones around the world use their smartphones to document atrocities.[1] In the process, they capture valuable evidence for war crimes prosecutions.[2] Until recently, this user-generated evidence was seen as a helpful but non-essential supplement to war crimes investigations.[3] That is no longer the case. Today, if an investigative team tried to build a war crimes case by considering evidence in only non-digital form, they would fail to meet the basic due diligence norms of their profession.[4]

A quirk of the digital evidence ecosystem is that much of the digital evidence generated globally is held by private U.S.-based social media companies.[5] Yet the U.S. legal frameworks that regulate the ability of platforms like Facebook, YouTube, or Twitter to share digital content are blind to the reality of today's international war crimes investigations. In 2021, the first test case

---

[1] *See* Rebecca J. Hamilton, *User-Generated Evidence*, 57 COLUM. J. TRANSNAT'L L. 1, 3–4 (2018) [hereinafter Hamilton, *User-Generated Evidence*] (discussing how increased mobile device accessibility contributes to more documentation of human atrocities).

[2] I use "war crimes" as the descriptor for the investigations/prosecutions/accountability efforts discussed in this Article not for its legal definition, but as colloquial shorthand for all the atrocity crimes under international law: war crimes, genocide, crimes against humanity, and aggression. Of course, crimes against humanity and genocide can occur in peacetime as well as during conflict, and the legal definition of war crimes does not encompass the other international crimes. *See* 18 U.S.C. § 2441 (defining conduct that constitutes a war crime as used in the U.S. Code). But "war crimes" in its colloquial sense captures the fact that the bulk of crimes this Article is concerned with take place in the midst of conflict or, in lay terms, war.

[3] *See* Hamilton, *User-Generated Evidence*, *supra* note 1, at 10–11 (tracing the history of the use of visual images in courtroom proceedings).

[4] As an indication of how quickly digital evidence is becoming institutionalized within these investigations, consider that the International Criminal Court (ICC) has recently published guidelines for those doing digital documentation in order to ensure that the material they record can be used in a subsequent ICC investigation. *See* INT'L CRIM. CT. OFF. THE PROSECUTOR, DOCUMENTING INTERNATIONAL CRIMES AND HUMAN RIGHTS VIOLATIONS FOR ACCOUNTABILITY PURPOSES: GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS (2022), https://www.icc-cpi.int/sites/default/files/2022-09/2_Eurojust_ICC_CSOs_Guidelines_2-EN.pdf (providing guidance to those doing digital documentation).

[5] *See generally infra* sections IV.A.–B. Of course, there is also plenty of digital evidence posted to non-U.S. platforms, in particular TikTok and Telegram. The issues involved in accessing digital evidence held by non-U.S. platforms is another pressing issue from a war crimes accountability perspective but is beyond the scope of this Article.

involving the effort to obtain digital evidence from a U.S. social media company for war crimes accountability made its way through U.S. courts.[6] The Republic of Gambia sought a court order to access digital evidence held by Facebook for use in an international case against Myanmar for genocide.[7] The result, which denied access to key pieces of digital evidence, was likely correct under the law as currently written.[8] From an accountability perspective, though, the outcome highlighted significant problems with the existing system for sharing digital evidence.[9]

The Biden Administration and the U.S. Congress—in a rare feat of bipartisan agreement—are committed to prioritizing war crimes accountability in light of the atrocities unfolding daily in Ukraine.[10] Yet those actually doing the work of seeking accountability face a legal framework that is obsolete for current needs. The troubling result, this Article argues, is a system that:

(1) Prohibits actors with the mandate and expertise to achieve international accountability from accessing digital evidence in the form of private content; and

---

[6] *See* Republic of Gambia v. Facebook, Inc., 575 F. Supp. 3d 8, 9 (D.D.C. 2021) (vacating, in part, the magistrate judge's original order requiring Facebook to disclose private accounts and content).

[7] *Id.* at 9.

[8] *See infra* section III.B. (noting current laws and how the Republic of Gambia's case was resolved).

[9] *See infra* section III.B.

[10] *See From Nuremberg to Ukraine: Accountability for War Crimes and Crimes Against Humanity: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. 1:31:30 (Sept. 28, 2022), https://www.judiciary.senate.gov/meetings/from-nuremberg-to-ukraine-accountability-for-war-crimes-and-crimes-against-humanity (statement of Sen. Lindsey Graham) (stating that financially supporting Ukraine and categorizing Russia as a state sponsor of terrorism are important steps, and "the other lane that we are interested in is letting the Russian military know that we are watching"); Jeff Mason & Simon Lewis, *Biden Says Putin Committed War Crimes, Calls Charges Justified*, REUTERS (Mar. 18, 2023, 5:12 AM), https://www.reuters.com/world/europe/us-says-no-doubt-russia-is-committing-war-crimes-ukraine-after-icc-issues-putin-2023-03-17/ (discussing President Biden's position regarding war crimes surrounding the events in Ukraine). For an indication of the significance of digital evidence to war crimes investigations in Ukraine, see Yousur Al-Hlou et al., *Caught on Camera, Traced by Phone: The Russian Military Unit that Killed Dozens in Bucha*, N.Y. TIMES (Dec. 22, 2022), https://www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html.

(2) Leaves accountability actors to request digital evidence in the form of removed-public and quasi-public content through an opaque system shaped by the financial, political, and cultural concerns of U.S. social media platforms.

The absence of a pathway through which international war crimes investigators can seek private content thwarts accountability for war crimes. Meanwhile, the system for seeking removed-public and quasi-public content grants immense discretion to U.S. social media companies, risking a scenario in which they share digital evidence with those pursuing accountability for favored victim groups, while simultaneously telling disfavored groups that U.S. law prohibits sharing digital evidence with them.

This Article argues that the law must be updated so that digital evidence sharing is permitted to achieve accountability for the major international crimes of genocide, war crimes, crimes against humanity, and aggression, with appropriate privacy protections and oversight. Future-proofing the law for the war crimes investigations of the coming decades is a major undertaking. It cannot—and probably should not—happen on a quick timeline. Given the rate at which technology is evolving, we should anticipate the sphere of digital evidence to expand beyond what we can currently imagine, let alone legislate for. The success of any future-proofing project will hinge, in large part, on establishing a legal framework for the digital era that has enough flexibility baked into it to allow the next generation to apply it to new technologies.[11]

In the short-term, however, there are discrete amendments to existing legislation that would address the immediate needs of those

---

[11] *See e.g.*, Kyriakos N. Kotsoglou & Marion Oswald, *The Long Arm of the Algorithm? Automated Facial Recognition as Evidence and Trigger for Police Intervention*, 2 FORENSIC SCI. INT'L: SYNERGY 86, 86 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7219190/ (arguing that Automated Facial Recognition technologies, when incorporated in investigative techniques and subsequent evidence in criminal proceedings, have the potential to revolutionize existing practices); Andrea Tundis, Humayun Kaleem & Max Mühlhäuser, *Detecting and Tracking Criminals in the Real World Through an IoT-Based System*, SENSORS, July 2020, at 1, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7374392/ (proposing a system based upon Internet of Things (IoT) social devices for detecting and tracking criminals); *see also* Brittan Heller & Daniel Castaño, *Artificial Intelligence, Virtual Courts, and Real Harms*, LAWFARE (Mar. 14, 2023), https://www.lawfareblog.com/artificial-intelligence-virtual-courts-and-real-harms

seeking accountability.[12] Any such reform must achieve two goals. First, the law must establish a transparent and principled basis for the disclosure of digital evidence so that such decisions are insulated from the arbitrary whims of financial, political, and cultural power. Second, the law must ensure that all disclosure is done in a way that upholds contemporary standards of privacy, data security, and civil liberties protections.

The Article proceeds as follows: Part II explains how U.S. social media platforms have inadvertently become major storage sites for digital evidence and delineates the broad categories of private, public, and quasi-public digital evidence. Part III introduces the legal landscape confronting those seeking digital evidence from U.S. social media companies. It first describes the major U.S. privacy law governing digital evidence disclosure: the Stored Communications Act (SCA), and its CLOUD Act amendments. It then summarizes 18 U.S.C. § 1782, which is the pathway through which parties to an international proceeding can seek evidence held in the U.S. and describes the *Republic of Gambia v. Facebook* (Meta) litigation, which was the first case to seek digital evidence disclosure from a U.S. social media company under § 1782. Part IV identifies the problems with the current system. It describes the mismatch between expertise and access produced by the system for the disclosure of private information. It then introduces, for the first time, material gleaned from interviews with accountability actors seeking to navigate the existing system for sharing removed-public and quasi-public content. This reveals the emergence of a concerning two-tier system for disclosure, the outcomes of which I situate within the past decade of content moderation scholarship on social media company decision-making. Part V turns to suggestions for reform, identifying complications with the effort to implement them. Part VI concludes.

II. U.S. SOCIAL MEDIA PLATFORMS AS EVIDENCE STORAGE SITES

Traditionally, the collection of war crimes evidence depended on professionals accessing the crime scene to obtain victim and witness

[12] *See infra* Part V.

testimony and collect physical evidence.[13] To the extent that perpetrators were state actors (or at least had the tacit support of their government) and were committing crimes in their own territory, it was common for the government to thwart accountability simply by denying investigators access to the crime scene.[14] As commercially available satellite imagery improved and became accessible to investigators, some visibility into the crime scene could be obtained without the consent of the government.[15] But this workaround was inherently limited to acts that took place outside of buildings and could be seen from a distance.[16]

The 2007 launch of the iPhone, and the range of cheaper alternatives that then flooded the market, radically changed the landscape for war crimes investigations. [17] For the first time, victims of atrocities could do their own documentation, and they frequently posted this user-generated evidence on the social media platforms that they were familiar with from their pre-conflict lives.[18] This meant that war crimes investigators—and indeed a much broader array of actors including journalists and human rights groups—gained visibility into areas they could not physically access.[19] It also

---

[13] *See* Hamilton, *User-Generated Evidence*, *supra* note 1, at 12 (providing a brief history of the use of visual evidence in court).

[14] For an extreme example, see Prosecutor v. Harun, ICC-02/05-01/07-48-Red, Prosecution Request for a Finding on the Non-Cooperation of the Government of the Sudan in the Case of The Prosecutor v. Ahmad Harun and Ali Kushayb, Pursuant to Article 87 of the Rome Statute, ¶ 49 (Apr. 19, 2010), https://www.icc-cpi.int/court-record/icc-02/05-01/07-48-red (claiming that the Sudanese government refused to cooperate with the ICC investigation into crimes in Darfur and threatened ICC investigators with death).

[15] *See e.g.*, *High Resolution Satellite Imagery and the Destruction of Housing Structures in Nehega, South Darfur*, AM. ASS'N FOR THE ADVANCEMENT SCI. (2011), https://www.aaas.org/resources/high-resolution-satellite-imagery-and-destruction-housing-structures-negeha-south-darfur (using satellite images to evaluate the location and extent of attacks in Nehega).

[16] *Id.*; *see also* Denise Chow & Yuliya Talmazan, *Watching from Space, Satellites Collect Evidence of War Crimes*, NBC NEWS (May 3, 2022, 4:13 AM), https://www.nbcnews.com/science/science-news/ukraine-satellites-war-crimes-rcna26291 (discussing using satellite images by war crime investigators).

[17] *See* Hamilton, *User-Generated Evidence*, *supra* note 1, at 3–4 (explaining that smart phones proliferated the footage of war crimes).

[18] *See id.* at 38 ("Users who record crime as it unfolds are witnesses to that crime. . . .").

[19] *See e.g.*, *Syria: Coordinated Chemical Attacks on Aleppo*, HUM. RTS. WATCH (Feb. 13, 2017, 10:57 AM), https://www.hrw.org/news/2017/02/13/syria-coordinated-chemical-attacks-aleppo (discussing Human Rights Watch's use of video uploaded by the Aleppo Media Center

meant, however, that social media platforms suddenly became major repositories of war crimes evidence.[20]

A. CATEGORIES OF CONTENT

The line between content that is public and content that is private is deceptively difficult to draw in practice given the wide array of privacy configurations available to users of social media platforms. For the purposes of this Article though, it is useful to simplify this reality by grouping content into one of three possible categories: private, public, and quasi-public. The following section takes the perspective of the originator of the content and uses a reasonable expectations standard to describe each category in turn. It also provides an overview of the content moderation systems run by social media companies that render public material invisible to platform users (and war crimes investigators).

1. Private Content. Private content is content that the originator of the content intended to share with a limited number of people of their choosing and no one else.[21] A classic example would be a user sending a message to another user on WhatsApp, Meta's end-to-end encryption messenger service.[22] While no system is foolproof from hacking, the user who sends the message can reliably expect that the person to whom they sent it will be the only person to see their message. For the purposes of this Article, examples of messages from one user to a limited number of other users sent through Direct Message on Twitter, or on Facebook Messenger, would also be considered private, even if end-to-end encryption were not enabled. Again, it is the reasonable expectation of most people using these services for one-on-one or small group conversations that the content of their communications is private.

---

to call attention to a February 2017 chemical weapons attack in Aleppo); *see also* Rebecca J. Hamilton, *Atrocity Prevention in the New Media Landscape,* 113 AJIL UNBOUND 262, 266 (2019) (explaining that because the new media landscape increases visibility it also increases attention from policymakers).

[20] *See, e.g.*, *Syria: Coordinated Chemical Attacks on Aleppo*, *supra* note 19 (presenting war crimes evidence produced through video recordings posted on social media).

[21] *Private Content Definition*, L. INSIDER, https://www.lawinsider.com/dictionary/private-content (last visited Feb. 13, 2023).

[22] *See* WHATSAPP, https://www.whatsapp.com (last visited Mar. 26, 2023) (describing WhatsApp as a private messaging system).

2. Public Content. Public content is content that a user posts to a social media platform with no restrictions on who can see it.[23] For the purposes of this Article, public material does not have to actually be seen by large numbers of people, or indeed seen by anyone; its public nature stems from the fact that the user posted it to a publicly accessible site, thus reasonably expecting that it would be publicly available. Crucially for war crimes investigations though, digital evidence that was once public under this definition can be removed (rendering it invisible to the public) through any of the content moderation processes described below.[24] From a privacy perspective, the removal of content from the view of the public does not move that content out of its public categorization; the user who posted it still intended for it to be publicly available. But it does mean that this public content is not visible to the public.

Content moderation systems are complex, and a full treatment of this area is unnecessary for the purposes of this Article.[25] But to understand the problems that this system creates for accountability actors, it is useful to have a basic overview of how content moderation operates, at least in relation to the digital evidence sought from social media companies, and it is to this that the following part turns.

3. Removed-Public Content: The Role of Content Moderation. When social media platforms first came into operation, there was no legal requirement for them to moderate the content that appears on their platforms.[26] They began to do so, however, out of a business

---

[23] *See Public Content Definition*, L. INSIDER, https://www.lawinsider.com/dictionary/public-content (last visited Feb. 13, 2023); Andrew Cohen, *Berkeley Law Center Creates First Global Protocol on Using Social Media as Evidence for War Crimes*, BERKELEY L. (Dec. 1, 2020), https://www.law.berkeley.edu/article/human-rights-center-berkeley-protocol-social-media-evidence-war-crimes-nuremberg/ (defining "public content" as photos, videos, and other content posted to social media sites).

[24] *See infra* section II.A.*3*.

[25] *See* Evelyn Douek, *Content Moderation as Systems Thinking*, 136 HARV. L. REV. 526, 531 (2022) ("[C]ontent moderation is a complex and dynamic system . . . .").

[26] *See, e.g.*, *Big Tech/Social Media Regulation: Section 230/Content Moderation*, TEX. L. (Sept. 30, 2022), https://tarlton.law.utexas.edu/c.php?g=1148742&p=8384171#s-lg-box-26622652 ("Section 230 of the federal Communications Decency Act, an important law in the debate over content moderation, provides immunity to Internet platforms from liability for the speech in which their users engage.").

imperative.[27] Platforms like Facebook, Twitter, and YouTube make the bulk of their profits through digital advertising that becomes more profitable the longer that users stay on their platforms.[28] And in the absence of moderation, online platforms rapidly become so inundated with spam and vile content that users do not feel safe being on them.[29]

Content moderation is best understood as a multilayered system, with design choices influencing what appears, and is amplified online, made well in advance of any content being posted.[30] For all major U.S. platforms, a pillar of this system is the set of community standards, or guidelines, they publish to explain what content they permit on their platforms. To take just two examples, Facebook prohibits "statements advocating for high-severity violence;"[31] YouTube prohibits "footage of corpses with massive injuries."[32]

Such standards make a great deal of sense from the perspective of making these platforms a safe and welcoming place for the typical user. But they become problematic for war crimes investigators.[33]

---

[27] *See* Kate Klonick, *The New Governors,* 13 HARV. L. REV. 1598, 1627–30 (2018) (describing the economic incentives behind content moderation).

[28] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT NEW FRONTIER OF POWER (2019) ("'Google maximizes the revenue it gets . . . by giving its best position to the advertiser who is likely to pay Google the most in total, based on the price per click multiplied by Google's estimate of the likelihood that someone will actually click on the ad.'" (quoting Peter Coy, *The Secret to Google's Success*, BLOOMBERG.COM (Mar. 6, 2006), https://www.bloomberg.com/news/articles/2006-03-05/the-secret-to-googles-success#xj4y7vzkg)).

[29] *See* James Grimmelmann, *The Virtues of Moderation*, 17 YALE J.L. & TECH. 42, 62 (2015) ("It only takes a few determined spammers or trolls to bring a discussion to a screeching halt.").

[30] *See* Douek, *supra* note 25, at 532 (arguing "for an approach to content moderation regulation based on systems thinking, which focuses on the ex ante institutional design choices involved in creating a system").

[31] *Facebook Community Standards: Violence and Incitement*, META (2023) [hereinafter *Facebook Community Standards*], https://transparency.fb.com/policies/community-standards/violence-incitement/.

[32] *YouTube Policies: Violent or Graphic Content Policies*, GOOGLE (2023), https://support.google.com/youtube/answer/2802008?hl=en&ref_topic=9282436.

[33] *See* Rebecca J. Hamilton, *Social Media Platforms in International Criminal Investigations,* 52 CASE W. RES. J. INT'L L. 213, 221–22 (2020) [hereinafter Hamilton, *Social Media Platforms*] ("It makes business sense for YouTube to preemptively remove anything that could potentially be reported as . . . war crimes . . . .").

Content "advocating for high-severity violence,"[34] for example, can be a valuable piece of evidence in proving the genocidal intent of a perpetrator. Once material is posted publicly online, it is possible for an investigator to save a copy and, using appropriate authentication procedures, secure it as digital evidence. Often, though, the most valuable digital evidence is removed from public view before it becomes accessible to an investigator. This can happen through one of the following pathways:

a. Algorithmic Removal

An increasingly large amount of content is removed before it ever appears publicly online, thanks to algorithmic screening. Machine-based content moderation "reads" content that users post and automatically screens out content that violates the standards the algorithm has been trained on.[35] Under pressure from regulators to keep their platforms free of terrorist propaganda, this form of automated removal is the most efficient means that platforms have of avoiding the hefty fines they incur if they let terrorist content appear online.[36] With this as the goal, however, machine-based content moderation is often over-inclusive in its removal of content; it sweeps up digital content to remove as terrorist propaganda even when it is, in fact, digital evidence from a war crimes perspective.[37]

b. User Flagging

The next layer of the content moderation system occurs when, notwithstanding the algorithmic removal described above, a social

---

[34] *Facebook Community Standards*, s*upra* note 31.

[35] *See* Rebecca J. Hamilton, *Platform-Enabled Crimes*, 63 B.C. L. REV. 1349, 1363 (2022) [hereinafter Hamilton, *Platform-Enabled Crimes*] ("The first layer of this defense system uses machine-based content moderation to 'read' posted content for prohibited material and screen it out automatically.").

[36] *See* Hamilton, *Social Media Platforms*, *supra* note 33, at 221 (discussing how a company failing to have more regulation could "face fines of up to 4% of their global turnover").

[37] *See, e.g.*, Bernhard Warner, *Tech Companies Are Deleting Evidence of War Crimes*, THE ATLANTIC (May 8, 2019), https://www.theatlantic.com/ideas/archive/2019/05/facebookalgorithms-are-making-it-harder/588931/ (describing a video that was quickly removed from Facebook which was evidence of a war crime).

media platform user sees content they believe violates the community standards of the platform.[38] The user can "flag" that content to the platform, requesting its removal.[39] In some cases, the flagged content will be automatically removed,[40] and in other cases it will be screened by a human content moderator, who determines whether to keep the content online.[41]

c. De-platforming

Social media companies proactively seek out content that violates their community standards but has nonetheless appeared online because it has slipped through the screening mechanisms described above.[42] This is what happened a year after the peak of the genocidal violence against the Rohingya in Myanmar. Although civil society groups had flagged content inciting genocide against the Rohingya as the atrocities were unfolding, flaws in Facebook's local interface meant that the reporting system did not work properly and much of the content remained online.[43] But in August 2018, a year after the peak of the atrocities, reports of Facebook's

---

[38] *See* Hamilton, *Platform-Enabled Crimes*, *supra* note 35, at 1363 ("The second layer relies on users to flag content that is prohibited . . . .").

[39] *See, e.g.*, *Flag and Fix Inappropriate Content*, GOOGLE, https://support.google.com/contributionpolicy/answer/7445749?hl=en (last visited Mar. 26, 2023) (describing how a user can flag Google reviews).

[40] *See, e.g.*, Marie Cartwright, *How to Stop Automated Flagging on Craigslist*, CHRON., https://smallbusiness.chron.com/delete-ad-facebook-campaign-44445.html (last visited Mar. 26, 2023) (noting that once a free ad on Craigslist receives a certain number of flags, it is automatically removed).

[41] *See, e.g.*, Juniper Downs, *Why Flagging Matters*, YOUTUBE OFF. BLOG (Sept. 15, 2016), https://blog.youtube/news-and-events/why-flagging-matters/ ("We have trained teams, fluent in multiple languages, who carefully evaluate your flags 24 hours a day, seven days a week, 365 days a year in time zones around the world. They remove content that violates our terms, age-restrict content that may not be appropriate for all audiences, and are careful to leave content up if it hasn't crossed the line.").

[42] *See* Hamilton, *Platform-Enabled Crimes*, *supra* note 35, at 1363 ("The final layer relies on human moderators to catch what the automated system misses and to review content that users have flagged.").

[43] *See id.* at 1364 (discussing how Myanmar's text encoding standard "rendered Facebook's reporting tool nonfunctional," thus human moderators had to inform Facebook of the genocidal content).

role in the violence hit U.S. media headlines.[44] And at that point Meta moved to de-platform content that had been posted by some of the alleged perpetrators of the genocide.[45]

To be clear, public content that has been removed from public view through any of the content moderation processes described above may not actually cease to exist. Often, social media companies—especially major ones like Facebook and YouTube—retain backup copies of the removed material, for varying lengths of time.[46] As a result, accountability actors must turn to the social media companies, now the repositories of the digital evidence, to gain access.

4. Quasi-Public Content. The final category of content serves as a catchall for material that is neither private nor clearly public. Content in this category falls along a wide spectrum. At one end, for example, one can picture a user who sets up a restricted Facebook Group that is only visible to the four members of their immediate family. The content on that page would be considered private for the purposes discussed here. At the other end of the spectrum is a Facebook Group with no restrictions on it. Between these two poles lie plenty of hard cases. Perhaps there is a Facebook Group that says it is for employees of a fire department. But if the owner of the Group allows anyone who says they are part of the fire department to join, without any verification mechanism in place, then it is hard to argue that the Group is private. Alternatively, imagine a Facebook Group where the owner only grants access to people who can provide an official identification document to show they have a Chinese surname. If the Group has 200 members, is it private? What about if it has one billion members? Similar questions can be posed for Facebook Pages and restricted Twitter accounts. Absent guidance that has yet to come from courts or legislatures, hard cases rest for now in the quasi-public category. It is a frustratingly ill-

---

[44] *See* Steve Stecklow, *Why Facebook Is Losing the War on Hate Speech in Myanmar*, REUTERS INVESTIGATES (Aug. 15, 2018), https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/ (providing a timeline of the violent speech on Facebook and why it took Facebook so long to remove the content).

[45] *See Removing Myanmar Military Officials from Facebook*, META (Aug. 28, 2018), https://about.fb.com/news/2018/08/removing-myanmar-officials/ (describing Facebook's action to remove accounts "engaging in coordinated inauthentic behavior on Facebook" in Myanmar).

[46] *See infra* note 87–89 (discussing *Gambia v. Facebook* and a dispute over the company's "backup" protection).

defined set. From the perspective of international investigators, though, its fuzziness matters less than one might imagine because under current U.S. law their access to both removed-public and quasi-public content alike is at the discretion of social media companies.[47]

III. LEGAL LANDSCAPE

The following part describes the legal landscape within which requests for access to digital evidence held by social media companies take place. The overarching legislation in this space is the Stored Communications Act (SCA).[48] Section III.A introduces the key features of the SCA as well as the amendments made to it through the 2018 CLOUD Act. Then it turns to how the SCA regulates access to private digital evidence on the one hand and removed-public and quasi-public evidence on the other. Section III.B introduces 28 U.S.C. § 1782, which enables U.S. courts to subpoena evidence held by U.S. persons to assist international courts and tribunals (or litigants before those forums). It is also currently the only means through which non-government actors can seek evidence held by U.S. social media companies when those companies decide not to disclose. The section concludes with a summary of the recent effort by The Gambia to obtain a 28 U.S.C. § 1782 discovery order to access digital evidence held by Facebook for the purposes of pursuing accountability from Myanmar at the International Court of Justice for genocide against its Rohingya population.

A. SCA/CLOUD ACT

The Stored Communications Act (SCA) was written long before social media existed and well before anyone imagined that these platforms would have such a central role in international accountability efforts.[49] Certainly, legislators did not, and could not have, foreseen that the rules they were writing would cover the

---

[47] *See infra* section III.A.*1*.

[48] 18 U.S.C. § 2702.

[49] *See id.* (showing the most recent version of the SCA, originally enacted in 1986).

disclosure of evidence that could be used to prosecute the perpetrators of serious international crimes.

The SCA protects digital communications by prohibiting platforms from sharing the content of user communications and placing tight controls around the U.S. government's ability to compel the disclosure of those communications.[50] The idea behind the original legislation was to extend Fourth Amendment protections to electronic communications that went through the hands of, or were stored by, third parties.[51]

There is an entire field of literature on the SCA, and criticism of the way that the legislation—written with an eye to the technology in play circa 1986—fails to comport with the realities of social media, is both prevalent and persuasive.[52] My focus here though, is on the parts of the legislation regulating access to digital evidence of genocide, war crimes, crimes against humanity, and aggression.

The SCA's bar on content disclosure is tempered only by a list of exceptions to the general prohibition.[53] The Act is structured such that social media platforms "*may* divulge the contents of a communication" when one of the exceptions listed under 18 U.S.C. § 2702(b) applies.[54] In other words, it provides a permissive standard that gives social media companies broad discretion over whether to disclose exception-category content.

From the perspective of international war crimes investigators, the most important among the exception-category material is the so-called implied consent exception, which permits—but does not require—social media companies to disclose content "with the lawful consent of the originator."[55] As discussed further below, courts have construed this to encompass material that was posted

---

[50] *See id.* (concerning the voluntary disclosure of customer communications or records).

[51] *See, e.g.*, 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, 1209–10 (2004) (noting that Congress intended the SCA to dictate the Fourth Amendment's protection of private Internet communications from third parties).

[52] *See, e.g.*, *id.* at 1214–16 (explaining how the SCA froze into law the "understandings of computer network use as of 1986" and, relatedly, how the Act fails to address many modern problems associated with Internet privacy).

[53] *See* Appendix.

[54] 18 U.S.C. § 2702(b) (emphasis added).

[55] § 2702(b)(3).

to a public site, even if it was subsequently made unavailable to the public through a content moderation process.[56]

The U.S. government can override a social media company's discretion by securing a warrant that compels the disclosure of any category of content.[57] Meanwhile, foreign governments that need access to digital evidence held by U.S. social media companies have traditionally had to work through a Mutual Legal Assistance Treaty (MLAT).[58] The MLAT process, however, is slow, cumbersome and not designed for an era in which so much evidence is in digital form.[59] In 2018, a pathway to a more efficient process opened as Congress worked on the Clarifying Lawful Use of Overseas Data (CLOUD) Act.[60]

Like the SCA, the CLOUD Act has been the subject of intense scholarly debate.[61] For the purposes of this Article however, the key

---

[56] *See supra* section II.A.*3*.

[57] *See, e.g.*, *Law Enforcement Online Requests*, FACEBOOK, https://www.facebook.com/records/login/ (last visited Mar. 26, 2023) (describing the process for the government to request Facebook records).

[58] As of April 2022, the U.S. government had sixty-eight bilateral MLATs with different States, in addition to one with the European Union. *Mutual Legal Assistance Treaties of the United States*, OFF. INT'L AFFS. CRIM. DIV. U.S. DEP'T JUST. (Apr. 2022), https://www.justice.gov/criminal-oia/file/1498806/download.

[59] *Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety,"* JUST. NEWS (Apr. 5, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-academy-european-law (describing the slow and cumbersome process of the MLAT and the need for reform).

[60] 18 U.S.C. § 2523.

[61] The background to the CLOUD Act lies in an effort by the U.S. government to obtain digital evidence held by Microsoft on a server in Ireland and challenged by Microsoft in U.S. courts. *See* Jennifer Daskal, Microsoft Ireland, *the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 9 (2018) ("Argued in February 2018, the Microsoft Ireland case presented the Court with a novel question resulting from changing technology and the rise of the cloud. Does a U.S. warrant, issued pursuant to the 1986 Stored Communications Act (SCA), reach emails and other communications content that are accessed and controlled by a U.S.-based company, but stored on a data server located outside the United States?"). On the eve of the U.S. Supreme Court deciding whether an SCA warrant issued by U.S. law enforcement could compel Microsoft to disclose content held on a server outside the U.S., Congress stepped in with the CLOUD Act. *See id.* ("On March 23, President Trump signed the CLOUD Act, thereby mooting one of the most closely watched Supreme Court cases this term: the *Microsoft Ireland* case." (footnote omitted)). The Act clarified that SCA warrants issued by U.S. law enforcement had extra-territorial reach. *See* Tim Cochrane,

feature of the CLOUD Act is its addition of a further exception to the SCA's prohibition on disclosure. The new exception enables access by foreign governments to content held by U.S. social media companies if the foreign government's purpose is the "prevention, detection, investigation, or prosecution of serious crime."[62] Disclosure is conditioned on the foreign government first having met a robust set of civil liberties, privacy, human rights, and data security requirements codified as § 2523 of the SCA.[63] The U.S. Attorney General, with the concurrence of the U.S. Secretary of State, must sign off on the satisfaction of these statutory requirements before the disclosure exception can come into play.[64] Once satisfied though, the foreign government can obtain the digital evidence they need directly from the social media company.[65]

Because international war crimes investigators have no authority to issue a search warrant, their ability to access digital evidence from a social media company varies based upon whether the content they seek falls inside the SCA's implied-consent exception. The graph below summarizes the system with respect to war crimes evidence.

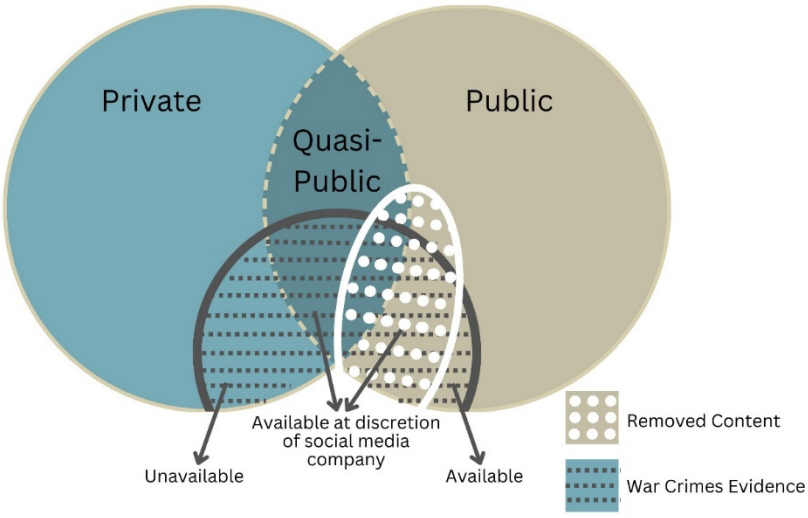
Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritorial Investigatory Powers, 32 DUKE J. COMP. & INT'L L. 153, 161 (2021) (noting that the CLOUD Act "confirmed Congress' intention to provide the SCA broad extraterritorial scope over data").

[62] 18 U.S.C. § 2523(4)(d)(i).

[63] § 2523(b)(1).

[64] § 2523(b).

[65] To date, however, the U.S. government has only certified these requirements with respect to the United Kingdom and Australia. Alex Grigsby, *The Intelligence Collection Implications of the CLOUD Act*, COUNCIL ON FOREIGN RELS. (Feb. 12, 2018), https://www.cfr.org/blog/intelligence-collection-implications-cloud-act.



Graph 1: Access to Digital Evidence for International War Crimes Investigators Under the SCA

As seen above, public content that has not been removed from a platform is accessible to war crimes investigators just as it is available to any other member of the public. By contrast, removed-public and quasi-public content is unavailable to war crimes investigators unless the social media company concerned has preserved the content and agrees to provide access to it. This is because the SCA gives social media companies discretion over whether to disclose content that is subject to the implied consent exception.[66] If the social media company decides not to disclose, the only recourse that war crimes investigators have available is to pursue a subpoena from a U.S. District Court under 18 U.S.C. § 1782.[67]

Turning to private content however, international investigators cannot gain access even when that content provides evidence of war

[66] § 2523(4)(d)(i).

[67] *See infra* section III.B.

crimes. In terms of actors who do have a pathway to accessing private content, the SCA permits U.S. government entities to obtain this content through the provision of a warrant.[68] And foreign governments can access private content if it relates to a "serious crime" either by working through an MLAT process (although this is widely considered too slow to be useful) or by establishing a CLOUD Act executive agreement with the U.S. government. Investigators at international courts or tribunals, though, have no pathway under the SCA through which to request access to private content.

B. 18 U.S.C. § 1782

For accountability actors who are neither U.S. law enforcement nor one of the foreign governments covered by the CLOUD Act provisions or an MLAT, the primary option for seeking digital evidence held by a U.S. social media company is to go to a U.S. District Court to pursue discovery under 18 U.S.C. § 1782. This provision enables a U.S. court to order a person (or corporation) in their jurisdiction to provide evidence in their possession to a foreign or international tribunal.[69] Any "interested person" can petition the court for such an order, which means this is a pathway that is not limited to prosecutors or other state officials; human rights groups and survivors of atrocities themselves are able to seek a § 1782 order.[70] Moreover, there is no requirement that the foreign or international tribunal case is a criminal proceeding, though if it is, then the petition can be for an investigatory use "before formal accusation."[71] Indeed, as the U.S. Supreme Court clarified in 2004, "[t]he 'proceeding' for which discovery is sought under § 1782(a) must be within reasonable contemplation, but need not be 'pending' or 'imminent.'"[72]

---

[68] § 2703.

[69] *See* § 1782 ("The district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal . . . .").

[70] *See* Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241, 256 (2004) ("The category of 'interested person' who can petition for a 1782 order 'plainly reaches beyond the universe of persons designated "litigant."'").

[71] 28 U.S.C. § 1782(a).

[72] *Intel Corp.*, 542 U.S. at 265.

A district court is not required to issue an order pursuant to a §1782 request, even if the statutory requirements are met. It can decline to issue an order on the basis of a number of discretionary considerations, including whether provision of evidence would be "unduly intrusive or burdensome."[73] The following describes the first case to seek a §1782 order for access to digital evidence held by a U.S. social media company. The Gambia—with no viable option to obtain information through an MLAT or the CLOUD Act—petitioned a U.S. District Court to obtain digital evidence held by Facebook for international proceedings related to the commission of genocide by Myanmar.

In November 2019, The Republic of The Gambia instituted proceedings against Myanmar at the International Court of Justice (ICJ).[74] The ICJ, based in The Hague, is an international court with jurisdiction to hear disputes between States.[75] The Gambia alleged that Myanmar had violated the UN Convention on Genocide, a treaty that both States have ratified.[76] The allegations arose from Myanmar's violent persecution of its minority Muslim population, the Rohingya, which led to the killing of thousands and displacement of hundreds of thousands of people.[77] The Gambia's case at the ICJ sought to hold Myanmar responsible under

---

[73] *Id.*

[74] *See The Gambia v. Facebook*, GLOB. FREEDOM EXPRESSION COLUM. UNIV., https://globalfreedomofexpression.columbia.edu/cases/gambia-v-facebook/ (last visited Mar. 26, 2023) ("In November, 2019, the Republic of The Gambia had initiated proceedings against Myanmar claiming breach of its obligations under international law on account of its ill treatment of the Rohingya minority.").

[75] *History*, INT'L CT. JUST., https://www.icj-cij.org/history (last visited Mar. 26, 2023).

[76] Application Instituting Proceedings and Request for Provisional Measures (The Gambia v. Myanmar), Pleading, ¶ 2 (Nov. 11, 2019) [hereinafter Gambia v. Myanmar Pleading], https://www.icj-cij.org/public/files/case-related/178/178-20191111-APP-01-00-EN.pdf.

[77] Human Rights Council, *Rep. of the Detailed Findings of the Indep. Int'l Fact-Finding Mission on Myan.*, U.N. Doc. A/HRC/39/CRP.2, ¶¶ 622–23 (2018) [hereinafter *HRC Rep. of the Detailed Findings*], https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf; *see* Press Release, United Nations Human Rights: Office of the High Commissioner, UN Expert Calls for Action Against Myanmar Military on Anniversary of Atrocities Against Rohingya, U.N. Press Release (Aug. 24, 2022), https://www.ohchr.org/en/press-releases/2022/08/un-expert-calls-action-against-myanmar-military-anniversary-atrocities (discussing the displacement of Rohingya survivors).

international law for the commission of genocide against the Rohingya.[78]

To prevail, The Gambia would have to show the Court that Myanmar officials committed acts of genocide, which includes showing that those acts were taken with the specific intent to destroy the Rohingya in whole or in part.[79] Showing specific intent is a notoriously challenging part of proving any allegation of genocide.[80] But in the case of atrocities committed against the Rohingya, there is a trove of digital evidence of intent because the Myanmar military used Facebook as a primary means through which to incite the genocide.[81]

The Myanmar military created scores of fake accounts through which to disseminate anti-Rohingya material to millions of Facebook users in Myanmar.[82] They posted the material publicly and coordinated through private groups and messages.[83] But much of the material that had been posted publicly was de-platformed by Facebook in late 2018, following a U.S. public outcry about the platform's role in the atrocities.[84] As a result, neither private postings nor previously public postings were accessible to The Gambia by the time it brought the case at the ICJ.

Against this backdrop, in June 2020, The Gambia sought a discovery order from the U.S. District Court for the District of Columbia under 28 U.S.C. § 1782 to obtain private, quasi-public,

---

[78] Gambia v. Myanmar Pleading, *supra* note 76, ¶ 15.

[79] *See* G.A. Res. 3/260, art. 2 (Dec. 9, 1948) ("[G]enocide means any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group . . . .").

[80] *See, e.g.*, Kai Ambos, *What Does "Intent to Destroy" in Genocide Mean?*, 91 INT'L REV. THE RED CROSS 833, 833 (2009) (arguing for the use of a lower knowledge-based standard with respect to lower level perpetrators); REBECCA HAMILTON, FIGHTING FOR DARFUR: PUBLIC ACTION AND THE STRUGGLE TO STOP GENOCIDE 38 (2011) (discussing the high bar posed by the specific intent standard in genocide investigations).

[81] *See HRC Rep. of the Detailed Findings*, *supra* note 77, ¶¶ 574–75 (discussing the Myanmar military's use of Facebook to incite hatred); *see also* Hamilton, *Platform-Enabled Crimes*, *supra* note 35, at 1351 (discussing the Myanmar military's use of Facebook to run a propaganda campaign against the Rohingya).

[82] Steve Stecklow, *Inside Facebook's Myanmar Operation Hatebook,* REUTERS (Aug. 15, 2018, 3:00 PM), https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

[83] *Id.*

[84] *See supra* notes 44–45 and accompanying text.

and removed-public digital evidence from Facebook for use in the ICJ proceedings.[85] Facebook opposed the request, arguing that "[a]bsent a statutory exception, the SCA strictly prohibits Facebook from disclosing the contents of communications on its platform in response to a civil subpoena like the one proposed here."[86]

Siding predominantly with The Gambia, in September 2021, the Magistrate Judge issued a subpoena requiring Facebook to disclose most of the material The Gambia requested.[87] In refuting Facebook's argument that the SCA prohibited such disclosure, the Court zeroed in on the language in § 2510(17)(B) of the SCA which prohibits disclosure of "any storage of such communication by an electronic communication service for purposes of *backup protection* of such communication."[88] Dealing with an issue of first impression as to the meaning of "backup protection" under the SCA, the Court concluded that removed content fell outside the meaning of "backup protection" because once the original posting was removed, the material preserved by Facebook was the only remaining version of the posting, and thus not a "backup."[89]

Once it was under a subpoena, Facebook backed away from its original claim that the SCA prohibits the disclosure of all material requested by The Gambia. It agreed to "produce to The Gambia public information that Facebook preserved from hundreds of accounts, groups, and pages removed from its platform in 2018 for

---

[85] Memorandum of Law in Support of the Republic of Gambia's Application for Order to Take Discovery Pursuant to 28 U.S.C. §1782 at 25, Republic of the Gambia v. Facebook, Inc. 575 F. Supp. 3d 8 (D.D.C. 2021), No. 20-mc-00036, https://storage.courtlistener.com/recap/gov.uscourts.dcd.218820/gov.uscourts.dcd.218820.1.1_1.pdf.

[86] Facebook's Opposition to Petitioner's Application Pursuant to 28 U.S.C. §1782 at 1, Republic of the Gambia v. Facebook, Inc., 575 F. Supp. 3d 8 (D.D.C. 2021), No. 20-mc-00036, https://storage.courtlistener.com/recap/gov.uscourts.dcd.218820/gov.uscourts.dcd.218820.8.0.pdf.

[87] *See* Republic of the Gambia v. Facebook, Inc., 567 F. Supp. 3d 291, 309 (D.D.C. 2021) ("Thus, outside of private messages, the content requested by The Gambia (as scoped to only include hate-speech and violent content) falls within the consent exception. Ordering discovery is particularly appropriate here because much of the requested content would have been publicly available to The Gambia had Facebook not deleted it.").

[88] 18 U.S.C. § 2510(17)(B) (emphasis added).

[89] *The Gambia*, 567 F. Supp. 3d at 303.

violating Facebook's terms of service."[90] Facebook explained that it felt it was able to disclose this de-platformed content under the implied consent exception to the SCA.[91] Facebook maintained, however, that the SCA prohibited it from disclosing other, non-public information sought by The Gambia.[92]

On appeal, the court vacated the Magistrate Judge's order with respect to (solely) private communications. Disagreeing that "backup protection" necessarily implied the existence of an original, the court found that the Magistrate Judge's understanding of "backup protection" was at odds with the legislative intent behind the SCA.[93] The rest of the Order, however, remains in place, and under subpoena, Facebook has now begun sharing removed-public content with The Gambia.[94]

IV. PROBLEMS WITH THE STATUS QUO

The following part assesses how the legal framework described above leads to several problems from the perspective of war crimes

---

[90] *See* Facebook's Reply to the Gambia's Response to Facebook's Objections to the Magistrate Judge's Order and Facebook's Opposition to the Gambia's Objections, at 1, *In re:* Application Pursuant to 28 U.S.C. § 1782, Republic of the Gambia v. Facebook, Inc., 575 F. Supp. 3d 8 (D.D.C. 2021), No. 1:20-mc-00036 [hereinafter Facebook's Reply] ("Facebook will produce public content and non-content metadata for hundreds of accounts affiliated with the Myanmar government that Facebook removed in 2018.").

[91] 18 U.S.C. § 2702(b)(3); *see* Transcript of Status Conference Before the Honorable Zia A. Faruqui, U.S. District Ct. Magistrate Judge, at 65–67, *In re*: Application Pursuant to 28 U.S.C. § 1782, Republic of the Gambia v. Facebook, Inc., 575 F. Supp. 3d 8 (D.D.C. 2021), No. 1:20-mc-00036 [hereinafter Status Conference Transcript] (arguing that the information was disclosable).

[92] Status Conference Transcript, *supra* note 91, at 119. The line between what is a "public" versus a "private" posting encompasses are large grey zone in relation to posts that have some restrictions but are nonetheless posted to a huge number of people. *See* discussion *supra* section II.A. The most fulsome discussion of this problem to date was undertaken in the California Supreme Court. *See* Facebook, Inc. v. Super. Ct., 417 P.3d 725, 749 n.37 (Cal. 2018) ("[W]hat is public under the SCA is not defined by what a social media provider labels as 'public.'").

[93] *See* Republic of the Gambia v. Meta Platforms Inc., No. 20-36 (D.D.C. Dec. 3, 2021), https://storage.courtlistener.com/recap/gov.uscourts.dcd.218820/gov.uscourts.dcd.218820.31.0.pdf (partially vacating the Magistrate Judge's original order).

[94] See *infra* notes 114–131 and accompanying text for a discussion of the uncertainty around what the SCA does and does not permit social media companies to share with respect to quasi-public content.

accountability. I describe first how the system for access to private content under the SCA means that accountability actors with the greatest expertise in war crimes investigations—international courts and tribunals— are the least able to access this type of digital evidence. I then turn to the challenges with the existing system for the disclosure of removed-public material and quasi-public content, drawing on the experiences of accountability actors seeking to navigate the disclosure of digital evidence. This reveals the immense discretionary power held by U.S. social media companies, from which we see the emergence of a concerning two-tier system for disclosure. I situate these observations within the past decade of content moderation scholarship on social media company decision-making.

A. THE MISMATCH OF EXPERTISE AND ACCESS

At present, only governments are able to access private content from U.S. social media companies. The U.S. government can pursue pathways available to it through § 2702(b)(7) of the SCA, and foreign governments can seek access either through an MLAT or, if their government has an executive agreement, through the CLOUD Act provisions.[95]

The SCA, therefore, enables governments to pursue international crime prosecutions in their domestic courts. From an atrocities accountability perspective, however, this incurs two major limitations. First, mass atrocity prosecutions are more commonly pursued through international rather than domestic courts. This is because the former have the mandate, jurisdiction, and expertise in this area that many domestic courts lack.[96] War crimes investigations are complex, involving massive amounts of evidence that require specialized expertise to analyze.[97] Second,

---

[95] As noted above, the number of foreign governments that can do this is miniscule, with only the United Kingdom and Australia having managed it thus far. For consideration of the implications of this on potential SCA reform for war crimes accountability purposes, see discussion *infra* Part V.

[96] *See, e.g.*, Hamilton, *Platform-Enabled Crimes*, *supra* note 35, at 1410 (describing the legal and practical challenges facing domestic courts seeking to pursue war crimes cases).

[97] U.S. courts obviously handle complex litigation all the time, but the U.S. record on the pursuit of war crimes prosecutions is abysmal. *See, e.g.*, Madison Bingle, *Holes in the United States "Never Again" Promise: An Analysis of the DOJ's Approach Toward Atrocity*

international law provides immunities that prevent high-level government officials from being prosecuted for serious crimes in domestic courts; these immunities do not apply in international courts.[98]

The net result is that for as long as the SCA permits only government officials to seek private content, rather than a broader category of actors, including prosecutors from international courts and tribunals, then the most complex mass atrocity cases, especially those involving crimes perpetrated or enabled by state officials, cannot be pursued.

B. PICKING FAVORITES

As illustrated by the white-dotted area in Graph 1, U.S. social media companies exercise unfettered discretion to disclose removed-public and quasi-public digital evidence.[99] It is important, then, to understand how they are using this discretion.

Over a six-month period in 2022, I sought interviews with Meta (Facebook), Twitter, and Google (YouTube) to gain their perspective on how the SCA works in practice, and how they were navigating requests for access to digital evidence by international investigators. Given the degree to which digital evidence held by Facebook is relevant to the Myanmar investigations, I tried repeatedly to speak with someone who could represent the company's position. In each case, I was told that they were "working on [my request]."[100] But, as of the time of publication, no one has yet agreed to speak with me.

I had better luck coming at the question from the perspective of war crimes investigators. In the Fall of 2022, I interviewed five current and former international investigators with experience seeking access to removed-public and quasi-public digital evidence held by U.S. social media companies relating to investigations of

---

Accountability, 73 ADMIN. L. REV. 869, 873–74 (2021) (explaining how the U.S. has yet to prosecute alleged violators of genocide or war crimes under its substantive laws).

[98] *See generally* Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium), Judgment, 2002 I.C.J.

[99] *See supra* section II.A.*1*.

[100] *See generally* Message from Iain Levine, Product Policy Manager for Human Rights, Meta (Dec. 6, 2022, 10:11 AM) (on file with author).

atrocities in Myanmar and Ukraine. I have removed identifying information at their request, so as not to risk jeopardizing current and future requests by themselves or their colleagues for access to digital evidence.

1. Investigator Perspectives. In March 2017, the UN Human Rights Council established a fact-finding mission to document alleged human rights violations being committed by the Myanmar military, the Tatmadaw,[101] against the minority Rohingya population.[102] In August 2018, that Mission concluded that "there is sufficient information to warrant the investigation and prosecution of senior officials in the Tatmadaw chain of command, so that a competent court can determine their liability for genocide."[103]

In late 2018, the UN Human Rights Council established an Independent Investigative Mechanism for Myanmar (IIMM)[104] to "collect, consolidate, preserve and analyse evidence of the most serious international crimes and violations of international law committed in Myanmar since 2011, and to prepare files in order to facilitate and expedite fair and independent criminal proceedings."[105]

Both the fact-finding mission and the IIMM sought digital evidence from Facebook, which had become "the internet" in Myanmar and had been used by the Tatmadaw to incite and coordinate atrocities.[106] As previously discussed, in 2019, lawyers for The Gambia also began asking Facebook for access to de-platformed content from Myanmar as they sought accountability for the genocide at the ICJ.[107]

---

[101] *See HRC Rep. of the Detailed Findings*, *supra* note 77, ¶ 71 ("Myanmar's political history has been heavily dominated by an all-powerful military, known as the Myanmar 'Tatmadaw', which has ruled the country for most of its existence.").

[102] *See id.* ¶ 6 ("The Independent International Fact-Finding Mission on Myanmar . . . was established by Human Rights Council resolution 34/22, adopted on March 24, 2017.").

[103] Human Rights Council, *Rep. of the Indep. Int'l Fact-Finding Mission on Myan.,* U.N. Doc. A/HRC/39/64, ¶ 87 (2018) [hereinafter *HRC Mission on Myan.*].

[104] *Independent Investigative Mechanism for Myanmar*, UNITED NATIONS, https://iimm.un.org (last visited Feb. 12, 2023).

[105] Human Rights Council Res. 39/2, U.N. Doc. A/HRC/RES/39/2, ¶ 22 (Sep. 27, 2018).

[106] *See HRC Mission on Myan.*, *supra* note 103, ¶ 74 ("Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the internet").

[107] *See supra* section III.B.*1.*

Investigators involved in requests by both the IIMM and The Gambia recount that engaging with Facebook was initially very challenging. "It took six months to even begin [making contact]," explained a former investigator with the IIMM.[108] "[Facebook's] initial position was that the SCA bars them from sharing [anything with us]," confirmed one of the investigators involved in The Gambia litigation.[109] "It wasn't until we told them they might be named in our report [that] they responded," observed the former IIMM investigator.[110]

In August 2020, following public condemnation of Facebook by the head of the IIMM, Facebook began disclosing digital evidence.[111] According to another investigator involved with the IIMM, this publicity was critical in getting Facebook to agree to disclose evidence. "They were looking really bad. I mean, not the kind of usual bad that social media companies look. But this was very specific. They went into Myanmar and made Facebook the Internet and within months of doing so their platform was being used to coordinate a genocide," he explained.[112]

By late 2021, Facebook was prepared to state before the U.S. District Court in The Gambia case that it would provide access to removed-public content, despite previously claiming that the SCA barred such disclosure.[113] I asked one of the investigators involved in the litigation what they thought of Facebook pointing to this as evidence of its commitment to international justice. "Now they're under a 1782 order and have to do it [and] they're spinning it as a selling point," he responded.[114]

---

[108] Interview with Investigator A (Nov. 9, 2022) (on file with author).

[109] Interview with Investigator E (Nov. 2, 2022) (on file with author).

[110] Interview with Investigator A, *supra* note 108.

[111] *See* Poppy McPherson, *Facebook Shares Data on Myanmar with United Nations Investigators*, REUTERS (Aug. 25, 2020, 2:14 PM), https://www.reuters.com/article/us-myanmar-facebook/facebook-shares-data-on-myanmar-with-united-nations-investigators-idUSKBN25L2G4 ("Facebook says it has shared data with United Nations investigators probing international crimes in Myanmar, after the lead investigator said the company was withholding evidence.").

[112] Interview with Investigator B (Oct. 28, 2022) (on file with author).

[113] *See* Facebook's Reply, *supra* note 90, at 1 ("Facebook will produce public content and non-content metadata for hundreds of accounts affiliated with the Myanmar government that Facebook removed in 2018.").

[114] Interview with Investigator E, *supra* note 109.

In terms of what categories of material Facebook is sharing with these accountability actors, the picture is quite opaque. Consistent with the SCA, Facebook is not disclosing private material.[115] That, however, is where the clarity ends. "Sometimes they construe something within the reach of the SCA, and other times they say the same kind of material is not within the SCA," explains one of the investigators.[116] "[T]hey say[,] 'we can give you what is not subject to the SCA'[—]but then that doesn't mean only what is public. There is this gray area."[117]

That gray area includes content in Facebook Groups. "Right now they're saying Groups are private. But we don't know. Some of those Groups might have 100,000 people in them at which point, are they really private?" asks an investigator working on the situation.[118] Another investigator explains that in some cases Facebook has shared pages from semi-restricted Groups.[119] A further aspect of uncertainty stems from whether the implied consent exception, which enables social media companies to share removed-public content under the SCA, also applies to removed-public content that originates from a bot (as opposed to a person).[120]

One of the investigators was sympathetic to the situation the social media companies face. "There are some things that just haven't been litigated so they are working without [legal] guidance," he pointed out.[121] He was frustrated, though, by having to work in the context of such opacity. "It is hard to tell where they've drawn the line [and] they won't put anything in writing," he explains.[122]

The experience for accountability actors working on the situation in Ukraine has been markedly different from the situation in Myanmar. One investigator who has worked across both situations began describing his efforts to secure cooperation from social media companies rather cryptically.[123] "They are willing to assist with

---

[115] *See* Investigator B, *supra* note 112 ("They're not going to give us anything that would be subject to a search warrant standard. No private messages for example.").

[116] *Id.*

[117] *Id.*

[118] Interview with Investigator E, *supra* note 109.

[119] Interview with Investigator B, *supra* note 112.

[120] Interview with Investigator C (Nov. 2, 2022) (on file with author).

[121] Interview with Investigator B, *supra* note 112.

[122] *Id.*

[123] Interview with Investigator C, supra note 120.

certain situations a little more freely," he told me.[124] I asked him to clarify what he meant by that.[125] "It's Ukraine," he responded.[126] I questioned whether this was across all the U.S. social media companies and he affirmed that yes, "[t]he big three of Meta, Twitter and Google move in a pack."[127]

This was confirmed by another investigator with experience trying to access evidence from social media platforms in other situations. She commented on how much easier it had been to get engagement from Meta, Twitter and Google regarding access to digital evidence since Russia's 2022 invasion of Ukraine.[128] In June 2022, Google hosted Twitter and Meta representatives on site at a meeting with accountability actors.[129] "They were very clear they were meeting because of pressure they were getting on Ukraine from the leadership within their companies," this investigator explained.[130] "Previously it had been the human rights people in the companies trying to move on this and not getting anywhere," she added.[131]

These are, to my knowledge, the only first-hand accounts in the literature of the experiences of accountability actors seeking digital evidence from social media companies. More research is required to draw any conclusive insights about how social media companies are exercising their discretion with respect to the disclosure for war crimes accountability. Yet the limited information garnered from these interviews does hint at the emergence of a two-tier system, driven primarily by considerations of social media company self-interest: liability, and reputation.

In situations where accountability actors come to a U.S. social media company buoyed by the realistic threat of legal liability or publicity that would be bad for the social media company's reputation, social media companies begin to share information that is within their discretion to disclose under the SCA. In a sense, there

---

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] Interview with Investigator D (Oct. 27, 2022) (on file with author).

[129] *Id.*

[130] *Id.*

[131] *Id.*

is nothing remarkable about this. These are profit-maximizing actors who one should expect would respond to external pressures that could affect their bottom line. A troubling consequence of their domination of significant parts of the twenty-first century's information ecosystem, however, is that it is these factors, rather than the gravity of the situation or other justice-oriented concerns, that determine which crimes—and ultimately victims—benefit from access to removed-public and quasi-public digital evidence.

2. Lessons from Content Moderation. The above interviews hint at the emergence of a two-tier system for the disclosure of digital evidence that is not driven by justice-oriented concerns, but rather by the self-interest of U.S. social media companies. These anonymized interviews alone cannot provide firm evidence of the phenomenon. Yet when placed in the context of the past decade of scholarship on the factors influencing social media companies' decision-making regarding what content to remove from their platform, these nascent observations point to familiar factors. This would seem to increase the likelihood that the observations arising from these interviews reflect the reality of the way that these social media companies exercise their discretion over what content they disclose, and to whom they disclose it.

Content moderation scholarship has repeatedly highlighted the pervasive influence of the particular profit model that underlies major U.S. social media platforms.[132] All major U.S. social media companies provide their platforms at no financial cost to their users.[133] Thus, rather than subscription fees, these platforms generate the majority of their revenues from surveillance-based advertising.[134] Under this model, greater profits are generated the longer that users stay on the platform. Social media companies have designed their newsfeed algorithms and content moderation systems by prioritizing the display of content that will sustain user engagement, thereby serving advertisers, even when such content fuels sectarian violence.[135] Against this backdrop, it would be

---

[132] *See* ZUBOFF, *supra* note 28, at 463–90 (providing an expansive critique of the advertising model on which Facebook is based).

[133] *See supra* Part II.

[134] *See* ZUBOFF, *supra* note 28, at 463–90 (noting and critiquing this model).

[135] *See* Hamilton, *Platform-Enabled Crimes*, *supra* note 35, at 1352 (describing the Facebook-fueled tragedy in Myanmar); *see also* Rebecca J. Hamilton, *Governing the Global*

unsurprising to learn that reputational threats that risk driving advertisers from the platform, such as the IIMM's public condemnation of Facebook, influence social media platforms' decision-making around digital evidence disclosure.[136]

The other consistent influence on U.S. social media company decision-making identified by the content moderation scholarship is the role of U.S. government soft power.[137] Over a decade ago, Yochai Benkler, then Co-Director of the Berkman Center for Internet and Society, studied the influence of the U.S. government over decision-making through a case study of the Wikileaks document disclosure. His case study highlighted "the influence of informal systems of pressure and approval on market actors."[138] He noted how these systems of pressure, despite being uncoordinated and indirect, enabled the U.S. government "to achieve, through a multi-system attack on critics, results that would have been practically impossible to achieve within the . . . requirements of legality."[139] Benkler's conclusions in relation to a range of online intermediaries down the Internet stack comports with scholarship specific to social media platforms, which has highlighted how the U.S. government can outsource its censorship goals to these private companies through informal and indirect means.[140]

Public Square, 62 HARV. INT'L. L.J. 117, 138–58 (2021) (describing atrocities in Myanmar, India, Sri Lanka, South Sudan, and Turkey).

[136] Since these interviews were conducted, the role that a negative reputation can play in deterring advertisers from associating themselves with a platform has been made abundantly clear following Elon Musk's controversial takeover of Twitter. *See* Halisia Hubbard, *Twitter Has Lost 50 of Its Top 100 Advertisers Since Elon Musk Took Over, Report Says*, NPR (Nov. 25, 2022), https://www.npr.org/2022/11/25/1139180002/twitter-loses-50-top-advertisers-elon-musk ("Half of Twitter's top 100 advertisers appear to no longer be advertising on the website.").

[137] *See*, *e.g.*, Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 312 (2011) (positing that the U.S. government can employ "new kinds of pressure" on social media companies to prevent unwanted disclosures); Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 863 (2012) (introducing the idea that "federal and state governments are increasingly using indirect methods to engage in 'soft' blocking of online material").

[138] Benkler, *supra* note 137, at 314.

[139] *Id.*; *see also* Bambauer, *supra* note 137, at 894 ("[I]nformal government pressures on key intermediaries accomplished what formal legal action likely could not.").

[140] *See* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298–99 (2014) (describing "public/private cooperation and co-aptation" as occurring when the State uses another entity to undertake its censorship goals); *see also* Danielle Keats

In light of the full-throated support of the U.S. government toward accountability for Russia's crimes in Ukraine, it seems predictable that social media company leadership would have engaged accountability actors on digital evidence from Ukraine, even as they have previously ignored similar requests for engagement in relation to other conflict situations. Without any of the social media companies involved being willing to speak to me, one is left to speculate about what exactly precipitated their proactive engagement with accountability actors on Ukraine in June 2022. This was the same month, however, that U.S. Attorney General, Merrick Garland, visited Ukraine to meet with the Ukrainian Prosecutor General and make a high-profile announcement that the U.S. "will pursue every avenue available to make sure that those who are responsible for these atrocities are held accountable."[141] Finally, it is important to situate Meta's response to requests for evidence from its platform in Myanmar within the litigation the company faces regarding its role in those atrocities, and in other conflict settings.[142] The Gambia sought material for the ICJ case against Facebook at the same time as Rohingya refugees brought suits in the U.S. and U.K. against the company for 150 million U.S. dollars, alleging it allowed the Myanmar military to incite genocide on its platform.[143] Again, with no comment available from Meta itself, one can only speculate about the impact that claim had on the company's willingness to share

---

Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1036–40 (2018) (introducing a discussion of the European Union's direct regulation of online speech, by contrasting the United States' failed attempts at direct regulation, and subsequent resort to indirect methods of influence).

[141] *See* Press Release, United States Department of Justice, Attorney General Merrick B. Garland Visits Ukraine, Reaffirms U.S. Commitment to Help Identify, Apprehend, and Prosecute Individuals Involved in War Crimes and Atrocities (June 21, 2022), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-visits-ukraine-reaffirms-us-commitment-help-identify (announcing the launch of a War Crimes Accountability team).

[142] *See* Rebecca Hamilton & Rosa Curling, *Facebook Beware: The "Rest of the World" Is Hitting Back*, JUST SEC. (Feb. 6, 2023), https://www.justsecurity.org/84982/facebook-beware-the-rest-of-world-is-hitting-back/ (discussing other litigation facing Facebook from around the world).

[143] *See* Dan Milmo, *Rohingya Sue Facebook for £150bn Over Myanmar Genocide*, THE GUARDIAN (Dec. 6, 2021), https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence (describing the two cases).

evidence that could potentially be used against it. The U.S. case by the Rohingya was recently dismissed, although the judge in the case left the door open for the plaintiffs to re-file.[144] Since then, however, other victims of crimes enabled by the Facebook platform in Ethiopia have sought 1.6 billion U.S. dollars in damages from the Kenya High Court.[145] A rudimentary conflict of interest analysis would suggest that Meta's discretion to decide whether to disclose evidence that could be used against it should, at a minimum, be closely monitored.

V. REFORM

As explained in the preceding sections, U.S. law poses two significant problems for international investigators seeking digital evidence from U.S. social media companies to prosecute genocide, war crimes, crimes against humanity or aggression. First, the SCA prohibits them from accessing private material, and neither the SCA nor any other piece of legislation provides a pathway through which they could overcome that prohibition, even in the most compelling circumstances. Second, their access to removed-public and quasi-public content is at the discretion of the social media companies. If a social media company chooses not to disclose digital evidence, the only recourse that international investigators have is to pursue costly and lengthy litigation through U.S. courts to compel the social media company to disclose under subpoena. International investigators are not equally placed when it comes to their ability to pursue such litigation given language barriers and access to the particular legal resources required. And even if they were, it is an additional and unnecessary hurdle to securing SCA-exempted digital evidence that Congress never set out to withhold from those pursuing accountability for the most serious international crimes. Most troublingly, a significant risk flowing from this arrangement is that evidence disclosure decisions are not being made in a

---

[144] Rachyl Jones, *The Rohingya's Genocide Suit Against Meta is Dismissed—For Now*, OBSERVER (Dec. 15, 2022, 8:37 AM), https://observer.com/2022/12/the-rohingyas-genocide-suit-against-meta-is-dismissed-for-now/.

[145] Constitutional Petition, Abrham Meareg v. Meta Platforms, Inc., L.L.R. (H.C.K. 2022) https://www.foxglove.org.uk/wp-content/uploads/2022/12/Constitutional-Petition-Abrham-Another-V-Meta.pdf.

consistent and principled manner, but are instead driven primarily by the self-interest of a few U.S. corporations, creating disparate outcomes across victim groups.

Bracketing for now the longer-term issues demanding legislative attention in this space, the following section describes two, non-exclusive, reforms: one focused on sharing of private content, the other on sharing of removed-public and quasi-public content. Both require additions to the existing list of disclosure prohibition exemptions under the SCA. Below I offer draft language for each additional exception to 18 U.S.C. § 2702, recognizing that such text is but a starting point for legislative discussion of the issue. Both proposed reforms seek to achieve the goals raised at the start of this article: to establish a transparent and principled basis for the disclosure of digital evidence, and to ensure that any disclosure upholds contemporary standards of privacy, data security, and civil liberties protections.

A. ACCESSING PRIVATE CONTENT

At present, U.S. social media companies are only permitted to share private content with a government entity, pursuant to a warrant from U.S. law enforcement (for U.S. government requests) or an order from a foreign government (per the CLOUD Act).[146] From a civil liberties standpoint, there are compelling reasons to keep the disclosure of private content highly circumscribed and tightly regulated. Indeed, many privacy advocates maintain that the CLOUD Act gave too much scope to foreign governments to obtain private content from U.S. social media companies.[147] Be that as it may, the CLOUD Act is now good law, and it has the virtue of requiring a foreign government to adhere to robust civil liberties and data protection standards before that government can access

---

[146] *See* 18 U.S.C. § 2703(a) (requiring disclosure "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); § 2702(b)(9) (allowing disclosure "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified")

[147] *See* CAMILLE FISCHER, THE CLOUD ACT: A DANGEROUS EXPANSION OF POLICE SNOOPING ON CROSS-BORDER DATA (Feb. 8, 2018), https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data (raising concerns that the CLOUD Act provisions for access by foreign governments were not as strong as U.S. warrant requirement protections).

private content in pursuit of accountability for a serious crime.[148] The following amendment to the SCA would do nothing more than extend this same possibility (with similar associated conditions and U.S. government oversight) to international courts and tribunals. The amendment to 18 U.S.C. § 2702 would read as follows:

> A provider described in subsection (a) may divulge the contents of a communication—
>
> (10) to a foreign government *or to an international court or tribunal investigating genocide, war crimes, crimes against humanity or aggression,* pursuant to an order from a foreign government *or international court or tribunal* that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § 2523.

Obviously, there would need to be an accompanying amendment to 18 U.S.C. § 2523 to incorporate international courts and tribunals within it. Tailoring such an amendment to the institutional characteristics of international courts and tribunals, as distinct from foreign governments, will not be straightforward.[149] Moreover, opening up the *possibility* of a CLOUD Act-type executive agreement to international courts and tribunals is by no means a guarantee that they will be able to successfully negotiate such an agreement with the U.S. Indeed, although that CLOUD Act opened up the possibility of such agreements to foreign governments in 2018, five years later only two countries have succeeded in reaching such an agreement.[150]

To some, the evident difficulty of meeting the 18 U.S.C. § 2523 pre-requisites to an executive agreement may seem like a bug, not

---

[148] *See* 18 U.S.C. § 2523 (conditioning data access agreements with foreign governments on certifications that "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement").

[149] *See infra* note 158 and accompanying text.

[150] *See supra* note 65 and accompanying text.

a feature of the CLOUD Act.[151] Yet in this case, given the relative inexperience that international courts and tribunals have in dealing with large volumes of digital evidence,[152] the conditions required by 18 U.S.C. § 2523 with respect to data security and privacy should be welcomed. Indeed, opening up the possibility of an executive agreement that would expedite digital evidence sharing, while conditioning that possibility on a rigorous set of security and privacy standards, would provide exactly the kind of incentive needed by international courts and tribunals to prioritize these issues in a world of limited resources.[153] The net result of this probably quite lengthy process will mean that U.S. social media companies are not put in the position of being asked to turn over digital evidence to entities that cannot properly secure it.

Finally, Congress would need to provide definitional clarity to the "international court or tribunal" language proposed here. In its most conservative form, the amendment could specify only the International Criminal Court in the first instance, then add other international courts and tribunals over time if the system is found to work well. Of course, a final check on claims by bogus entities would be provided by a CLOUD Act requirement that any international court or tribunal must be certified by the U.S. Attorney General. However, definitional clarity on the front end by Congress would safeguard against the risk of the U.S. Attorney General being inundated with frivolous claims from newly created entities cynically trying to fashion themselves as "international

---

[151] *See infra* section V.C. (outlining the potential complications with meeting and enforcing the § 2523 preconditions).

[152] *See* Chelsea Quilling, *The Future of Digital Evidence Authentication at the International Criminal Court*, J. PUB. & INT'L AFFS. (May 20, 2022), https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court ("While new technology holds great promises in transforming the judicial process related to international crimes in many ways, the Court is presently underprepared to undertake the complex tax of authenticating and verifying digital evidence.").

[153] *See* Lindsay Freeman & Rachel Vazquez Llorente, *How to Prepare the International Criminal Court for Our Digital Age*, OPINIOJURIS (Dec. 10, 2021), https://opiniojuris.org/2021/10/12/how-to-prepare-the-international-criminal-court-for-our-digital-future/ ("The magnitude of potential evidence . . . in the Information Age, paired with the limited budget and resources upon which the ICC operates, requires a delicate balancing act between the prosecutor's duty to investigate and the efficiency of the proceedings.").

courts" (and perhaps at the behest of authoritarian regimes) to gain access to private content.

B. ACCESSING REMOVED-PUBLIC OR QUASI-PUBLIC CONTENT

The SCA permits but does not require social media companies to disclose digital evidence in situations where the person posting the content consented, such as by posting the content publicly.[154] The practical import of this implied-consent exception in the SCA is that social media companies have discretion to disclose removed-public and quasi-public content to international investigators for war crimes accountability.[155]

There is nothing to stop social media companies moving toward a transparent and principled system for the disclosure of digital evidence themselves by creating and publishing their own guidelines on the topic.[156] Indeed, this would be welcomed by international war crimes investigators currently struggling to navigate an opaque and inconsistent disclosure system.[157] In addition, however, (and especially in light of Meta's initial reaction to The Gambia litigation) it may be useful for Congress to clarify that whenever digital evidence is needed for an international

---

[154] *See* 18 U.S.C. § 2702(b)(3) ("A provider . . . *may* divulge the contents of a communication—with the lawful consent of the originator . . . ." (emphasis added)); *see also* Republic of the Gambia v. Facebook, Inc., 567 F. Supp. 3d 291, 308 (D.D.C. 2021) (relying on the rule that one implicitly consents to disclosure of a post when one has a reasonable basis to believe that information could be made public).

[155] *See* 18 U.S.C. § 2702(b) (allowing, but not requiring social media companies to reveal the content of communications). I bracket for now the question of where the lines are between private v. public content; in other words, how far the implied-consent exception extends. Clarifying the scope of the implied-consent exception is essential in order to reduce the quantity of material falling into the indeterminate quasi-public category, but it is an endeavor that will take time given the growing variety of privacy restrictions available to users. Moreover, given the possible future permutations that could confound any effort to determine the types of content that fall within the implied-consent exception today, any legislative work in the space would need to build in enough flexibility to allow new types of content to be added as technology evolves.

[156] *See e.g.*, *Information for Law Enforcement Authorities: International Legal Process Requirements*, META, https://transparency.fb.com/policies/improving/working-with-law-enforcement/ (last visited Apr. 23, 2023) (exemplifying the lack of transparency in digital evidence disclosure guidelines for international disputes).

[157] *See supra* notes 114–131 and accompanying text.

proceeding regarding a serious international crime, the SCA is not a barrier to compliance by a social media company. Such an amendment to 18 U.S.C. § 2702(b) would read as follows:

> A provider described in subsection (a) may divulge the contents of a communication—
>
> (11) *for the purposes of supporting international accountability investigations or prosecutions for genocide, war crimes, crimes against humanity or aggression, carried out by an international court, tribunal, or mechanism.*

Given the range of actors such an amendment would encompass, and the associated privacy and data security risks that come with disclosure, any such exception would need to include an accompanying amendment to specify that private (as opposed to public or quasi-public) content could only be received by entities with a CLOUD Act-type executive agreement certified by the U.S. Attorney General.

C. COMPLICATIONS

As foreshadowed above, the proposed reform to increase access to private content by offering international courts and tribunals the possibility of a CLOUD Act type executive agreement is not straightforward. The preconditions to a CLOUD Act agreement listed in 18 U.S.C. § 2523 were written for foreign governments, with U.S. government interests in mind. Of course, some of these can be applied in a near cut-and-paste fashion to international courts and tribunals. For example, although international courts and tribunals do not face the same obligations under international law as states, they could be required to meet amended standards that are broadly analogous to those in 18 U.S.C. § 2523 in relation to the prevention of cybercrime, and the assurance of data security and human rights.[158] Meanwhile, other requirements become

[158] *See* 18 U.S.C. § 2523(b)(1)(B)(i) (preventing cybercrime); *see also* § 2523(b)(1)(B)(iv) (assuring data security); § 2523(b)(1)(B)(iii) (assuring human rights).

nonsensical when applied to an international court or tribunal, and these could just be set aside.[159]

Certain preconditions, however, raise much thornier issues. For example, 18 U.S.C. § 2523(b)(4)(A) demands that a foreign government "may not intentionally target a United States person or a person located in the United States."[160] For many, if not all international courts and tribunals, it may be impossible for them to make such a commitment given their constitutional obligations to the equal pursuit of justice without discrimination based on nationality.[161]

More broadly, the institutional design of a foreign government is markedly different from most international courts and tribunals with respect to the capacity for oversight of data retention practices.[162] In a government context, executive action can be reviewed by a court of general jurisdiction.[163] Alternatively, oversight of the collection, retention, and use of data required by 18 U.S.C. § 2523(b)(1)(B)(iv) could be done by an independent agency with expertise in data security. In the context of an international court or tribunal, action can be overseen by a court, but it is a court with expertise in international criminal law. What experience international courts have had with digital evidence is very recent, and they have yet to develop expertise in data security.[164] The pre-conditions listed in the CLOUD Act assume the existence of a

---

[159] *See* § 2523(b)(1)(B)(vi) (finding it hard to see how a court could demonstrate a commitment to "the open, distributed, and interconnected nature of the Internet").

[160] § 2523(b)(4)(A).

[161] *See* Rome Statute of the International Criminal Court, art. 21, § 3, July 17, 1998, 2187 U.N.T.C. 90 ("The application and interpretation of law pursuant to this article must be consistent with internationally recognized human rights, and be without any adverse distinction founded on grounds such as gender as defined in article 7, paragraph 3, age, race, colour, language, religion or belief, political or other opinion, national, ethnic or social origin, wealth, birth or other status.").

[162] I would like to express my gratitude to Asaf Lubin for a particularly helpful conversation on this point.

[163] *See* JOHNATHAN M. GAFFNEY, CONG. RSCH. SERV., R46738, EXECUTIVE ORDERS: AN INTRODUCTION 8 (2021) (detailing that courts may review executive actions).

[164] *See* Rebecca J. Hamilton, *New Media Evidence Across International Courts and Tribunals, in* BEYOND FRAGMENTATION: CROSS-FERTILIZATION, COOPERATION AND COMPETITION AMONG INTERNATIONAL COURTS AND TRIBUNALS 113 (Giorgetti & Pollack, eds., 2022) (discussing that "[t]his type of evidence is now starting to make its way into international courts and tribunals").

capable independent actor to oversee orders that an authorized foreign government makes of a U.S. social media company. If legislators proceed down this path in order to increase access to private content for international courts and tribunals, then much thought will need to be given to fundamental institutional design differences between these international bodies and foreign governments.

In addition, there is a political challenge arising, in part, from the extant silo-ing of the war crimes accountability community from the privacy community. Major privacy advocates, notably the Electronic Frontier Foundation, fought hard against the passage of the CLOUD Act because it fell short of the procedural safeguards required for a warrant.[165] In the end, the CLOUD Act passed; the privacy protections and data security standards required under 18 U.S.C. § 2523 were enough to get the legislation "over the line" politically. But it is reasonable to assume that it would be near-impossible to convince privacy advocates, and their Congressional allies, to accept any digital evidence-sharing pathway that did not meet at least the standards set out in 18 U.S.C. § 2523. To date, those in the war crimes accountability community have made little effort to convince their counterparts in the privacy community of the need to increase access to digital evidence for serious international crimes.[166] Privacy advocates are likely to be worried that governments (primarily, but perhaps not exclusively, authoritarian ones) will try to manipulate any amendment offered to international courts and tribunals to harm the privacy interests of their citizens.[167] Their concerns are not ill-founded, but they can also not be used as a trump card that ends the conversation on the need for reform. Those in the war crimes accountability community

---

[165] *See* Camille Fischer, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*, ELEC. FRONTIER FOUND. (Feb. 8, 2018), https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data (raising concerns that the CLOUD Act does not limit the scope of applicable crimes, provide notice to any parties involved, or meet sufficient standards comparable to warrant review).

[166] *See* discussion *supra* section IV.A.

[167] *See* Sarah Repucci & Amy Slipowitz, *The Global Expansion of Authoritarian Rule*, FREEDOM HOUSE (Feb. 2022), https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule ("Authoritarian regimes have become more effective at co-opting or circumventing the norms and institutions meant to support basic liberties . . . .").

must both make the case for reform *and* advance the reform conversation in a way that is mindful of the important privacy implications that will flow from it.

In light of all these challenges, it is worth reiterating that there is nothing to stop social media companies moving proactively to address at least one of the two problems raised in this Article. The SCA has vested U.S. social media companies with extraordinary discretion over the disclosure of removed public and quasi-public content, some of which has now become essential for the prosecution of the most serious international crimes. Legislative reform may be delayed due to political and/or technical reasons. But it is clear that Congress never intended to enable U.S. social media companies to use the SCA as a bar to the disclosure of removed-public and quasi-public evidence that could be useful in the prosecution of genocide, war crimes, crimes against humanity, or aggression.[168] Legislators were simply unaware, back when they drafted the SCA, that the Act would come to cover such material.[169]

Against this backdrop, U.S. social media companies should develop and publish their own interim guidelines on how they make evidence disclosure decisions with a presumption in favor of the disclosure of removed public and quasi-public evidence needed for the pursuit of accountability for the international crimes of genocide, war crimes, crimes against humanity, and aggression. If or when courts or legislators move to define the lines between private and public content for the purposes of SCA disclosure, then the interim guidelines could be amended to reflect those definitions. In the meantime, having at least interim guidelines against which external actors could evaluate the disclosure decisions being made by these companies would start to introduce some much-needed consistency and oversight into this shadowy realm of decision-making.

---

[168] *See* discussion *supra* section III.B.

[169] *See* JIMMY BALSER, CONG. RSCH. SERV., LSB10801, OVERVIEW OF GOVERNMENT ACTION UNDER THE STORED COMMUNICATIONS ACT (SCA) 1 (2022) (explaining that the SCA was passed in 1986 "to address government wiretaps and other communications tracing issues").

VI. CONCLUSION

This Article has identified a serious conflict between the needs of war crimes investigators pursuing accountability in the digital era and U.S. laws regulating access to digital evidence. Legislators never set out to create this conflict; it arose as the result of laws written in an era when the scale and importance of digital evidence to present-day accountability efforts was simply unimaginable. Now though, with the problem squarely before them, legislators have the responsibility to begin the long process of future-proofing U.S. laws to support accountability in the digital era. The way in which social media ecosystems have evolved has given U.S. law an outsized role in determining the prospects for justice in crimes committed far outside the U.S., including those involving no U.S. citizens whatsoever. It is incumbent on Congress to be mindful of these global implications as they consider how to improve these laws.

While this Article has proposed two discrete amendments to facilitate the flow of evidence to accountability actors in the short-term, future-proofing U.S. laws for the coming era is a much bigger undertaking. An initial step towards this larger goal would be for legislators to convene a study group, or task the Department of Justice and the State Department's Office for Global Criminal Justice with researching the issue, and provide a report on their findings to Congress.[170] Outside of government, the war crimes accountability community and privacy advocates need to start working together to sensitize each other to their respective concerns and lay the groundwork for future legislative changes. And courts, tribunals, and investigative mechanisms working on war crimes accountability need to strengthen their data security protocols as a matter of urgency if they want to access digital evidence held by U.S. companies.

Ultimately, the entire information-sharing system needs revamping to future-proof it, not just for digital evidence held by social media companies but also for the array of technologies,

---

[170] There is ample precedent for such a tasking. *See e.g.*, H. Amendment 262 to H.R. Res. 7900, 117th Cong. (2022) (directing the "FBI, Department of Homeland Security, and the Secretary of Defense to publish a report that analyzes and sets out strategies to combat White supremacist and neo-Nazi activity in the uniformed services and Federal law enforcement agencies not later than 180 days after enactment and every six months thereafter").

including much that we cannot yet imagine, that will be vital to the work of accountability for atrocities going forward. In this respect, an incremental approach, with scope for adaptation at each step, is the soundest route to take.

VII. APPENDIX: EXCEPTIONS TO THE PROHIBITION ON DISCLOSURE UNDER 18 U.S.C. § 2702

(b) Exceptions for disclosure of communications.—A provider described in subsection (a) may divulge the contents of a communication—

> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
>
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
>
> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;
>
> (7) to a law enforcement agency—
>
> (A) if the contents—
>
> (i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.