PLATFORMS, ENCRYPTION, AND THE CFAA: THE CASE OF WHATSAPP V. NSO GROUP

Jonathon W. Penney[†] *& Bruce Schneier*[††]

ABSTRACT

End-to-end encryption technology has gone mainstream. But this wider use has led hackers, cybercriminals, foreign governments, and other threat actors to employ creative and novel attacks to compromise or workaround these protections, raising important questions as to how the Computer Fraud and Abuse Act (CFAA), the primary federal anti-hacking statute, is best applied to these new encryption implementations. Now, after the Supreme Court recently narrowed the CFAA's scope in *Van Buren* and suggested it favors a code-based approach to liability under the statute, understanding how best to theorize sophisticated code-based access barriers like end-to-end encryption, and their circumvention, is now more important than ever.

In this Article, we take up these very issues, using the recent case *WhatsApp v. NSO Group* as a case study to explore them. The case involves a lawsuit launched in 2019 by WhatsApp and Facebook against the cybersecurity firm NSO Group, whose spyware has been linked to surveillance of human rights activists, dissidents, journalists, and lawyers around the world, as well as the death of *Washington Post* journalist Jamal Khashoggi. The lawsuit, brought under the CFAA, alleged NSO Group launched a sophisticated hack that compromised countless WhatsApp users—many of which were journalists and activists abroad. Despite these broader human rights dimensions, the lawsuit's reception among experts has been largely critical. We analyze WhatsApp's CFAA claims to bring greater clarity to these issues and illustrate how best to theorize encrypted platforms and networks under the CFAA. In our view, the alleged attack on WhatsApp's encrypted network *is* actionable under the CFAA and is best understood using what we call a network trespass theory of liability. Our theory and analysis clarifies the CFAA's application, will lead to better human rights accountability and privacy and security outcomes, and provides guidance on critical post-*Van Buren* issues. This includes setting out a new approach to theorizing the scope and boundaries of computer systems, services, and information at issue, and taking the intended function of code-based access barriers into account when determining whether circumvention should trigger liability.

DOI: https://doi.org/10.15779/Z384B2X554

† Research Fellow; Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University. The author played no part in the WhatsApp v. NSO Group lawsuit, nor any research it is based on.

†† Fellow and Lecturer, Belfer Center for Science and International Affairs, Harvard Kennedy School; Fellow, Berkman-Klein Center for Internet and Society, Harvard University.

TABLE OF CONTENTS

I. INTRODUCTION

Encryption has gone mainstream.[1] Now, after the Snowden and Cambridge Analytica scandals showed there is a demand for it, smartphone manufacturers and social media companies have increasingly sought to employ encryption to ensure users' privacy and security.[2] For example, popular social media messaging applications like WhatsApp, Facebook Messenger, Apple's iMessage, Snapchat, and Zoom, among many others, all

1. Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 990 (2018).

2. Naomi Colvin, *Whistle-Blowing as a Form of Digital Resistance*, 7 STATE CRIME J. 24, 27 (2018) ("In making the covert visible, Edward Snowden's revelations about mass surveillance also produced a recognition that there is a market for communications privacy. The proliferation of encrypted messaging applications and moves towards ubiquitous web encryption is a significant example of technical self-help against pervasive passive surveillance."); Steven H. Hazel, *Privacy Self-Help*, 36 BERKELEY TECH. L.J. XX, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3623569 (noting "millions" of consumers engage in privacy self-help now, including using encrypted messaging apps); Ken Kantzer, *Yet Another End-To-End Encrypted App*, PKC SECURITY (Dec. 16, 2016), https://www.pkcsecurity.com/yet-another.html ("It seems that every week, yet another end-to-end encrypted app is unleashed on the world . . . ."); Ariel Mahlmann, *End-to-End Encryption Strategies Becoming the Norm for Social Media*, FORNETIX (January 24, 2019), https://blog.fornetix.com/end-to-end-encryption-strategies-becoming-the-norm-for-social-media.

now implement end-to-end encryption or plan to do so in the near future.[3] End-to-end encryption is a type of secure communications that ensures messages are entirely encrypted while in transit so only the sender and the recipient have the special cryptographic keys to decrypt and view communications; to anyone else, including the network or platform operators themselves, they are indecipherable.[4] In this way, end-to-end encryption acts as both a code-based barrier—protecting the content of communications from all third parties—and an authentication gate, as only the sender and recipient have the keys to decrypt and view each message. There is also an important human rights dimension to these developments. Social justice activists at home[5] and human rights activists and dissidents abroad increasingly use end-to-end encrypted messaging applications like Signal and WhatsApp to protect themselves from government and corporate surveillance, malicious hackers, and cybercriminals alike.[6]

3. Mahlmann, *supra* note 2; Dylan Clarke & Syed Taha Ali, *End to End Security is Not Enough*, *in* SECURITY PROTOCOLS 260, 261 (Frank Stajano, Jonathan Anderson, Bruce Christianson & Vashek Matyáš eds., 2017); Catalin Cimpanu, *Zoom backtracks and plans to offer end-to-end encryption to all users*, ZDNET (June 17, 2020), https://www.zdnet.com/article/zoom-backtracks-and-plans-to-offer-end-to-end-encryption-to-all-users/.

4. *See A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?*, ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE GUIDE (Nov. 19, 2018), https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work; Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/; Leonid Grinberg, *End-to-End Authentication: A First Amendment Hook to the Encryption Debate*, 74 N.Y.U. ANN. SURV. AM. L. 173, 180–85 (2018); Mahlmann, *supra* note 2. For example, WhatsApp's end-to-end encryption ensures only the sender and recipient can see communications—not any third parties, including other WhatsApp users or WhatsApp administrators themselves. *See About End-to-End Encryption*, WHATSAPP, https://faq.whatsapp.com/general/about-end-to-end-encryption (last visited Aug. 12, 2021).

5. Amelia Nierenberg, *Signal Downloads Are Way Up Since the Protests Began*, N.Y. TIMES (June 11, 2020), https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html.

6. *See* Colvin, *supra* note 2, at 35 (stating the UN Special Rapporteur for Freedom of Expression has also advocated for legal protections for encryption); Amelia Nierenberg, *Signal Downloads Are Way Up Since the Protests Began*, N.Y. TIMES (June 11, 2020), https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html; *Encryption is for "Real People"*, HUMAN RIGHTS WATCH DISPATCHES (Aug. 2, 2017), https://www.hrw.org/news/2017/08/02/encryption-real-people ("Who else uses end-to-end encryption? The list is long. Peaceful pro-democracy and reform activists in places like Hong Kong, Turkey, Central Africa, and across the Middle East. LGBT people living in countries where their sexual orientation is criminalized. Whistleblowers who reveal governmental or corporate malfeasance. Journalists everywhere trying to protect their sources. Add to that list diplomats and government officials, including some in the UK parliament and Foreign Office. Or doctors, lawyers, and business people discussing sensitive and confidential information.").

But this wider use of encryption, especially in popular communications applications and networks, has led both governments and hackers to employ creative and novel methods to circumvent or "workaround" these protections, like exploiting encryption vulnerabilities or backdoors,[7] or targeting communication network "endpoints" with malware and spyware.[8] These activities raise important questions as to how the Computer Fraud and Abuse Act (CFAA), the primary federal anti-hacking statute, best applies to end-to-end encrypted networks and attempts to circumvent it. In fact, the issue has taken on even greater urgency in light of the United States Supreme Court's recent landmark decision in *United States v. Van Buren*.[9] The Court at long last endorsed a "narrow reading" of the CFAA, confirming it is "fundamentally" a trespass statute.[10] That is, the "basic wrong" leading to

7. JEFF KOSSEFF, CYBERSECURITY LAW 336 (2020); Kerr & Schneier, *supra* note 1, at 1006; Nicole Perlroth, *What Is End-to-End Encryption? Another Bull's-Eye on Big Tech*, N.Y. TIMES (Nov. 9, 2019), https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html ("[S]ecurity experts noted that any back door created for United States law enforcement agencies would inevitably become a target for foreign adversaries, cybercriminals and terrorists.").

8. Clarke & Ali, *supra* note 3, at 261; Megan Squire, *End-to-End Encryption Isn't Enough Security for "Real People"*, SCI. AM. (Aug. 15, 2017), https://www.scientificamerican.com/article/end-to-end-encryption-isn-rsquo-t-enough-security-for-ldquo-real-people-rdquo/.

9. Van Buren v. United States, 141 S. Ct. 1648 (2021).

10. Orin Kerr, *The Supreme Court Reins In the CFAA in Van Buren*, LAWFARE BLOG (June 9, 2021), https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren ("[T]his is a major victory for those of us who favor a narrow reading of the CFAA. It settles that the CFAA is fundamentally a trespass statute. The basic wrong is bypassing a closed gate, going where you're not supposed to go. The CFAA does not make it a crime to break a promise online. It does not make it a crime to violate terms of service. The statute is all about gates: When a gate is closed to a user, the user can't wrongfully bypass the gate."); *see also* Aaron Mackey & Kurt Opsahl, *Van Buren is a Victory Against Overbroad Interpretations of the CFAA, and Protects Security Researchers*, EFF DEEPLINKS BLOG (June 3 2021), https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security; *Van Buren: The implications of what is left unsaid*, IAPP PRIVACY ADVISOR (June 18, 2021), https://iapp.org/news/a/van-buren-the-implications-of-what-is-left-unsaid/; Will Duffield, *Van Buren Decision Is a Step in the Right Direction*, CATO INST. BLOG (June 14, 2021), https://www.cato.org/blog/van-buren-decision-step-right-direction; Clifford R. Atlas, Jonathan L. Crook, Jason Christopher Gavejian, Joseph John Lazzarotti & Erik J. Winton, *Supreme Court Adopts Narrow Interpretation of Computer Fraud and Abuse Act*, MARTINDALE LEGAL LIBR. (June 4, 2021), https://www.martindale.com/legal-news/article_jackson-lewis-pc_2546923.htm; Debbie L. Berman, David Bitkower, April A. Otterberg, Shoba Pillay, Aaron R. Cooper, Andrew J. Plague & Eric Fleddermann, *SCOTUS Limits the Reach of the Computer Fraud and Abuse Act, with Implications for Cybersecurity, Trade Secrets Litigation, and Beyond*, LEXOLOGY (June 6, 2021), https://www.lexology.com/library/detail.aspx?g=25ca11d7-1dff-4a69-a256-030b97c4cbca; Tiana Demas, Kathleen Hartnett, John Hemann, Travis LeBlanc, Joseph Mornin & Darina Shtrakhman, *US Supreme Court Narrows Scope of Computer Fraud and Abuse Act in Van Buren, Remands LinkedIn*, COOLEY

criminal and civil liability under the CFAA is bypassing an access barrier—or "gate"—in order to access, or go where you are not supposed to go, on a computer system or network.[11] Though the Court did not entirely settle what qualifies as a gate, it is clear the Court favors code-based or technological access restrictions—like end-to-end encryption.[12] Additionally, the Court cast considerable doubt on the usefulness of the CFAA in regulating and policing insider threats—those with authorization or permission to access a computer system or network—like an employee, contractor, or social media platform user who has created a free account.[13] Insider threats have long been a central cybersecurity concern,[14] especially in an era of ubiquitous computing and social media.[15] Using what the Court called a "gates up-or-down inquiry," if a

CYBER/DATA/PRIVACY INSIGHTS (June 9, 2021), https://cdp.cooley.com/us-supreme-court-narrows-scope-of-computer-fraud-and-abuse-act-in-van-buren/.

11. *See Van Buren*, 141 S. Ct. at 1651–58, 1661–62; Kerr, *supra* note 10; *see also* Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10. Certain leading scholars have long argued trespass law is key to understanding the CFAA. *See, e.g.*, Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146 (2016) ("[C]oncepts of authorization rest on trespass norms."); Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016); Michael J. O'Connor, *The Common Law of Cyber-Trespass*, 85 BROOK. L. REV. 421, 434–35 (2019).

12. In footnote 8 of *Van Buren*, the Court appears to leave open the possibility that contract and policy-based access restrictions can lead to CFAA liability despite rejecting the policy-based *use* restrictions at issue in the case. *See* 141 S. Ct. at 1658 n.8; *see also* Kerr, *supra* note 11; Orin Kerr (@OrinKerr), TWITTER (June 3, 2021, 8:10 PM), https://twitter.com/OrinKerr/status/1400500114569916422 (concluding that *Van Buren* likely requires a "mostly technological test, but one that can be impacted by written restrictions"); Paul Ohm (@Paul Ohm), TWITTER (Jun. 3, 2021, 5:57pm), https://twitter.com/paulohm/status/1400466767290400784 ("I think footnote 8 is a red herring and just forestalls the eventual 'code-based' approach in some future opinion. It's hard to read the rest of the opinion without thinking Barrett is gesturing requiring code-based."); Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

13. The Court called them "inside hackers." *Van Buren*, 141 S. Ct. at 1658.

14. Indeed, most cybercrime is committed by "insiders." *See* Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1493 (2016) (noting in Table 4 that well over half of cybercrime was committed by a combination of employees, consultants, and contractors, users or customers, and business partners); Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA HIGH TECH. L.J. 177, 184 (2000) ("According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes."); *see also* LUCAS WRIGHT, PEOPLE, RISK, AND SECURITY 40–43 (2017) (discussing insider threats).

15. Popular social media and communications platforms (like Facebook, Twitter, or WhatsApp) typically have hundreds of millions, even billions, of users—a target rich environment for malicious actors—and are generally accessible to anyone with an internet connection. *See* Marianna Noll, *Insider Threats on Social Media*, IT SECURITY CENTRAL (November 7, 2017), https://itsecuritycentral.teramind.co/2017/11/07/insider-threats-on-social-media/ ("Consider how much compromising information people share on social media which can include personal life details, political views, location, interests, and much

user has any authorized access to a computer system ("gates up") then there is no CFAA liability for violating *use* restrictions—like those found in terms of service or use policy—that regulate improper uses of the network or information therein to which they have access.[16] Previously, if terms of service or use policies prohibited such activities—such as abusing access to target other users, misappropriating information for malicious purposes, or carrying out attacks or other illicit activities against targets elsewhere online—some courts found that insiders could be liable under the CFAA for exceeding their authorized access.[17] Not anymore. Now, the only way an insider can exceed authorized access is when they access information—such as "files, folders, or databases," etc.—in other "areas within the [computer] system," to which they had no access to begin with.[18]

After *Van Buren*, understanding and theorizing the nature and scope of sophisticated code-based access barriers and authentication gates—like end-to-end encryption—under the CFAA is now more important than ever, as

more. For cyber criminals this data about a target is an absolute goldmine. . . . More than sharing information, social media platforms also provide another vector for phishing and drive-by-installations of malware. In either case social media platforms become a threat to your organization, which cannot be ignored if you allow your employees to use their social media at work."); Ellen Messmer, *Hackers use corporate attacks as staging grounds for other cyber assaults*, NETWORK WORLD (Mar. 1, 2013), https://www.networkworld.com/article/2164029/hackers-use-corporate-attacks-as-staging-grounds-for-other-cyber-assaults.html; Guerrino Mazzarolo, Juan Carlos Fernández Casas, Anca Delia Jurcut & Nhien-AnLe-Khac, *Protect Against Unintentional Insider Threats: The risk of an employee's cyber misconduct on a Social Media Site*, in CYBERCRIME IN CONTEXT 79–82 (M. Kranenbarg & Leukfeldt eds., 2021); *see also* Helen Margetts, *Rethinking Democracy With Social Media*, *in* RETHINKING DEMOCRACY 107–08 (Andrew Gamble & Tony Wright eds., 2019) ("Social media—digital platforms which allow the creation, location and exchange of content—are entwined with every democratic institution and the daily lives of citizens, having reached incredible levels of penetration. Worldwide, Facebook has 2 billion users, YouTube has 1.5 billion, Whats-App 1.2 billion, Instagram 700 million, Twitter 328 million and the Chi-nese WeChat 889 million; nearly three quarters (73 per cent) of US adults use YouTube, while 68 per cent use Facebook.").

16. *Van Buren*, 141 S. Ct. at 1651–58, 1661–62; Kerr, *supra* note 10; Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

17. There was a significant Circuit split before *Van Buren*. This broader interpretation of the CFAA—that breaching use policies could lead to liability—was held by the First, Fifth, Seventh, and Eleventh Circuits. The "narrow interpretation" of the CFAA, employed by the Second, Fourth, and Ninth Circuits, largely held that CFAA liability requires something more than a mere use restriction violation, like those found in terms of service or use policies. *See* KOSSEFF, *supra* note 7, at 176–83; Jonathan Mayer, *The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying United States v. Nosal*, 84 GEO. WASH. L. REV. 1644, 1646, 1657–58 (2016).

18. *Van Buren*, 141 S. Ct. at 1651–59, 1662; Kerr, *supra* note 10; Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

well as efforts to circumvent them by insiders with network access.[19] But just as important is the task of theorizing different kinds of computer systems, and information therein, under the CFAA to understand what it means for users to exceed authorized access by accessing "information" in "other areas" within a "computer system."[20] Theorizing the nature of the computer system and the misappropriated information at stake has always been an important issue under the CFAA,[21] but after *Van Buren*, it is now central to any CFAA liability analysis, particularly concerning hackers with authorized access to a network. Yet, this is an issue that courts have often failed to address seriously or systematically.[22]

In this Article, we take up these very issues, using a recently launched lawsuit *WhatsApp v. NSO Group*,[23] as a case study to explore them. The lawsuit was brought by WhatsApp Inc. and its parent company, Facebook, pursuing multiple CFAA claims against the cybersecurity firm NSO Group and its parent company Q Cyber Technologies (hereinafter "Complaint").[24] The Complaint, filed in California, alleged among other things that in 2019, NSO Group exploited a vulnerability in WhatsApp in order to spy on and monitor WhatsApp users, violating several provisions under the CFAA. WhatsApp CEO Will Cathcart, in launching the suit, declared it was part of the company's efforts to "protect the privacy and security of our users

19. Bryan Cunningham, John Grant & Chris Jay Hoofnagle, *Fighting Insider Abuse After Van Buren,* LAWFARE BLOG (June 11, 2021), https://www.lawfareblog.com/fighting-insider-abuse-after-van-buren; Timothy Edgar, *Why Van Buren Is Good News for Cybersecurity*, LAWFARE BLOG (August 4, 2021), https://www.lawfareblog.com/why-van-buren-good-news-cybersecurity.

20. Atlas et al., *supra* note 10 (noting that the key inquiry under the CFAA involves determining whether an individual had authorized access to the "areas of a computer system at issue"); Cunningham, Grant & Hoofnagle, *supra* note 19.

21. Mayer, *supra* note 17, at 1651–53 (observing that "order to properly evaluate these theories of liability, a court must necessarily sketch the boundaries of the computer system and the information and services that the defendant accessed"); Orin S. Kerr, *Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1653 (2003).

22. Mayer, *supra* note 17, at 1651–53 (noting that "courts have not seriously defined the scope of a computer system"); Kerr, *supra* note 21, at 1653 (noting the *Morris* case "raised questions about how to divide a network of computers into individual computers for the purpose of the statute," though those issues were ignored by the Second Circuit on appeal).

23. Complaint & Demand for Jury Trial at 1, WhatsApp, Inc. & Facebook, Inc. v. NSO Grp. Technologies Ltd. & Q Cyber Technologies Ltd., No. 3:19-cv-07123, 2015 WL 1033734 (N. D. Cal. Oct. 29, 2019) [hereinafter Complaint].

24. *Id.* at 11–13.

everywhere."[25] Indeed, the case has important implications for privacy, security, and human rights, and not just due to WhatsApp's massive 1.6 billion active user base.[26] NSO Group's Pegasus spyware tool has been directly linked to surveillance of human rights activists, dissidents, journalists, and lawyers in countries around the world—often by governments with poor human rights records—as well as the death of *Washington Post* journalist Jamal Khashoggi.[27] More recently, the Pegasus Project, publicized by Amnesty International, documented 50,000 Pegasus spyware targets—via methods that echoed the 2019 attack on WhatsApp users—linking NSO Group to the surveillance of countless heads of state, human rights activists, and journalists globally, including Jamal Khashoggi's family..[28] But the case also goes to the heart of ambiguities as to how encrypted networks, like WhatsApp's end-to-end encryption service, are best theorized under the CFAA, a salient issue given the broad range of online service providers and platforms now incorporating this technology. Moreover, the FBI is investigating NSO Group for CFAA violations due to the WhatsApp hack, which means criminal proceedings may also follow regardless of what happens in the civil litigation.[29]

25. Will Cathcart, *Why WhatsApp is pushing back on NSO Group hacking*, WASH. POST (Oct. 29, 2019), https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/.

26. Simon Kemp, *Digital 2020: Global Digital Overview*, DATAREPORTAL (Jan. 30, 2020), https://datareportal.com/reports/digital-2020-global-digital-overview.

27. Many such links have been made via research by the Citizen Lab, based at the University of Toronto's Munk School of Global Affairs and Public Policy. *See NSO Group*, CITIZEN LAB, https://citizenlab.ca/tag/nso-group/ (last visited Sept. 17, 2021) (supplying links to reports and related media); *see also* Nina dos Santos & Michael Kaplan, *Jamal Khashoggi's private WhatsApp messages may offer new clues to killing*, CNN (Dec. 4, 2018), https://www.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html.

28. Stephanie Kirchgaessner, *Officials who are US allies among targets of NSO malware, says WhatsApp chief,* THE GUARDIAN (July 24, 2021), https://www.theguardian.com/technology/2021/jul/24/officials-who-are-us-allies-among-targets-of-nso-malware-says-whatsapp-chief ("Cathcart said that he saw parallels between the attack against WhatsApp users in 2019 – which is now the subject of a lawsuit brought by WhatsApp against NSO – and reports about a massive data leak that are at the centre of the Pegasus project");Press Release, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*, AMNESTY INT'L (July 18, 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/; Ben Hubbard, *Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia*, N.Y. TIMES (Jan. 28, 2020), https://www.nytimes.com/2020/01/28/reader-center/phone-hacking-saudi-arabia.html.

29. Joseph Menn & Jack Stubbs, *Exclusive: FBI probes use of Israeli firm's spyware in personal and government hacks—sources*, REUTERS (Jan. 30, 2020), https://www.reuters.com/article/us-usa-cyber-nso-exclusive/exclusive-fbi-probes-use-of-israeli-firms-spyware-in-personal-and-government-hacks-sources-idUSKBN1ZT38B.

Despite these broader human rights dimensions, the lawsuit's reception among experts has been largely critical. It has been derided as an exercise in public relations,[30] and the lawsuit's CFAA claims criticized by various legal and cyber-security experts as "muddled,"[31] unclear, and "odd."[32] Critics also argue the lawsuit's claims rely too heavily on terms of service (TOS) violations,[33] contrary to the "narrow interpretation" of the CFAA then employed by various Circuit Courts of Appeal, and recently endorsed by the Supreme Court in *Van Buren*.[34] But perhaps the most serious charge is that the lawsuit asserts a problematic interpretation of the CFAA. It alleges NSO Group is liable for exceeding authorized access to the WhatsApp messaging network not because the network was hacked or exploited but because it was the staging ground and conduit through which the Defendants carried out their alleged attack on WhatsApp users.[35] This "theory" of the CFAA claims, critics allege, is akin to arguing you need Google's permission before sending an email through Gmail's network servers.[36] If correct, they argue, then the internet itself is in trouble—it would mean CFAA liability every time a server, host, or network is used without permission or for activities not

30. Jamie Condliffe, *The Week in Tech: WhatsApp's Spyware Fight Is at Least Good P.R.*, N.Y. TIMES (Nov. 1, 2019), https://www.nytimes.com/2019/11/01/technology/whatsapp-nso.html.

31. Tor Ekeland, *What's Up with WhatsApp: Thoughts on the NSO CFAA Complaint*, TOR EKELAND L. BLOG (Oct. 30, 2019), https://www.torekeland.com/whats-up-with-whatsapp-thoughts-on-the-nso-cfaa-complaint/.

32. Condliffe, *supra* note 30 (quoting Susan Landau calling it "odd"); Newsroom, *Facebook Enters Uncharted Legal Waters With Spyware Suit*, FORDHAM L. NEWS (Nov. 1, 2019), https://news.law.fordham.edu/blog/2019/11/11/facebook-enters-uncharted-legal-waters-with-spyware-suit/ (describing it as "risky").

33. *See* Andy Greenberg, *WhatsApp's Case Against NSO Group Hinges on a Tricky Legal Argument*, WIRED (Oct. 29, 2019), https://www.wired.com/story/whatsapp-nso-group-lawsuit/ (interviewing Tor Ekeland).

34. *See* Mayer, *supra* note 17, at 1646, 1657–58; KOSSEFF, *supra* note 7, at 176–78.

35. Josephine Wolff, *Whatever You Think of Facebook, the NSO Group Is Worse*, N.Y. TIMES, (Nov. 6, 2019), https://www.nytimes.com/2019/11/06/opinion/whatsapp-nso-group-spy.html ("WhatsApp does its best to argue that NSO gained access to its own signaling and relay servers without authorization in the process of contacting WhatsApp users, but this is a dicey interpretation of the Computer Fraud and Abuse Act, akin to arguing that you need Google's permission to send an email to a Gmail user through Google's servers"); Ekeland, *supra* note 31 (arguing the Complaint reads as if there was "unauthorized access" because the Plaintiffs "didn't like the way their network was used" and insisting that "if that's the standard for CFAA liability . . . then most of the internet is in trouble").

36. Wolff, *supra* note 35.

authorized by administrators or owners.[37] Such a broad interpretation of the CFAA is, they argue, "dicey,"[38] "risky,"[39] and "dangerous."[40]

We analyze WhatsApp's CFAA claims to bring greater clarity to these issues and illustrate how best to theorize encrypted networks and attacks on them under the CFAA. On the facts of the case, a fairly straightforward application of the CFAA would find that the Defendants were liable to targeted WhatsApp users for accessing their devices without authorization, using the WhatsApp network as a conduit to deliver malicious code to the victims' smartphones that allowed the Defendants unauthorized access. In fact, that is the basis for much of the criticisms of the lawsuit—the targeted users were the proper plaintiffs. The harder question, which we tackle in this Article, is whether WhatsApp, the company, also has a CFAA claim against the Defendants for their alleged attack on WhatsApp's encrypted messaging network. In our view, it does, based on what we call a network trespass theory.[41] This theory of liability is simple. It holds accessing a network and using it to hack or stage an attack on users of that network—like obtaining unauthorized access to their personal computing devices using malicious code over the network—is a trespass not just on the individual devices of the targeted users, but on the network itself, and should attract liability under the CFAA.

This theory involves subtle two legal and theoretical shifts. First, we argue for a different theoretical understanding and scope of the "computer system" at issue here—WhatsApp's encrypted communications network. Rather than theorizing user devices—through which users interface with the network via a software client—as separate computer systems, we argue they ought to be treated as constitutive of the same network for the purposes of determining CFAA liability. Typically, we think of computer networks—like the internet—as simply a series of interconnected but separate computers.[42]

37. *See* Ekeland, *supra* note 31; Wolff, *supra* note 35.

38. Wolff, *supra* note 35.

39. Newsroom, *supra* note 32.

40. *See* Tim Cushing, *Malware Marketer NSO Group Looks Like It's Blowing Off Facebook's Lawsuit*, TECHDIRT (Jan. 15, 2020), https://www.techdirt.com/articles/20200109/11485043708/malware-marketer-nso-group-looks-like-blowing-off-facebooks-lawsuit.shtml; *see also* Alan Z. Rozenshtein, *The WhatsApp-NSO Group Lawsuit and the Limits of Lawful Hacking*, LAWFARE BLOG (Nov. 5, 2019), https://www.lawfareblog.com/whatsapp-nso-group-lawsuit-and-limits-lawful-hacking.

41. The theory is based on norms of trespass law as applied to certain kinds of online networks. *See* Kerr, *supra* note 11, at 1146 ("[C]oncepts of authorization rest on trespass norms."); O'Connor, *supra* note 11, at 434–35; *see generally* Goldfoot & Bamzai, *supra* note 11.

42. MICROSOFT COMPUTER DICTIONARY 12 (4th ed. 1999) (defining it as "[a] group of computers and associated devices that are connected by communications facilities . . . .");

Hence, critics of *WhatsApp v. NSO Group* lawsuit claim the *real* victims of the hack are the users whose personal devices—separate computers from the WhatsApp network—were compromised and accessed. We argue this assumption makes sense for open networks like the internet but not encrypted networks like WhatsApp. End-to-end encrypted networks are not analogous to the open internet. They are closed networks with a central code-based design feature—end-to-end encryption—built into the network to protect the privacy and security of users and their communications. And users and their personal computing devices are not separate from the network, but, as the end nodes of the network that initiate, encrypt, send, receive, and decrypt calls, messages, and other user files and information shared over the network—essentially, all the core network functions—they are central to the network. As such, the scope and boundaries of the computer system here—the WhatsApp network—are best theorized as including users and their devices. Second, we argue that in deciding whether a code-based access barrier or authentication gate is circumvented or violated, courts should take into account the code-based access barrier's *intended function* in a computer system or network. Leading scholars have long argued that the best way to approach code-based access restrictions is as authentication gates,[43] and there are passages in *Van Buren* suggesting the Supreme Court may favor such an approach.[44] But, we argue, construing code-based access barriers so narrowly may mean certain kinds of sophisticated attacks that "work around" stronger code-based barriers like encryption, in ways unrelated to authentication functions, may not trigger liability. To catch those too, we suggest that the *intended function* of the code-based barrier in a computer system or network should be taken into account, and where access is outside authentication or *inconsistent with the intended function of the authentication gate or code-based access barrier*, then the circumvention should trigger liability.

Analyzed through the lens of this network trespass theory, the facts alleged in the lawsuit support multiple violations under the CFAA. Our network trespass theory clarifies the CFAA's application to communications networks. It is also consistent with the CFAA's underlying trespass norms, ultimately avoids reliance on terms of service violations, and, we argue, should lead to better privacy and security outcomes in the long term. Second,

DICTIONARY OF COMPUTING 5 (6th ed. 2008) (defining it as "the shared use of a series of interconnected computers, peripherals and terminals").

43. Kerr, *supra* note 11, at 1146; Kerr, *supra* note 10.

44. Van Buren v. United States, 141 S. Ct. 1648, 1651–59, 1662 (2021); Kerr, *supra* note 10; Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

the lawsuit helps fill a gaping void both domestically and internationally—a means to hold companies accountable for contributing to human rights abuses abroad. Lastly, though the WhatsApp lawsuit provides the foundation for our analysis, our arguments have implications far beyond it, providing guidance not just for FBI's reported investigation of NSO Group for criminal CFAA violations, but also on critical post-*Van Buren* issues: theorizing the nature and scope of "computer systems" and "areas"—like encrypted communications networks and similar platforms—and how best to theorize sophisticated code-based measures like end-to-end encryption, and efforts to bypass it, under the CFAA.

Our analysis has two caveats. First, though the factual allegations in the Complaint are not yet proven—and NSO Group has disputed them in court filings[45]—for the purposes of this Article, we assume the allegations set out are true. We also rely on some additional facts and research concerning WhatsApp's vulnerability that were not pleaded in the action. Second, we also focus primarily on the CFAA legal claims set out in the Complaint. A fuller analysis of other issues—like WhatsApp's claims under California state law or NSO Group's jurisdictional arguments and sovereign immunity claims[46]—would take us beyond the scope of this Article. However, our arguments have implications for WhatsApp's claims under California's Comprehensive Computer Data Access and Fraud Act and trespass law,[47] in addition to possible criminal violations being presently investigated. In Part II, we set out the central factual and legal claims in the lawsuit and then set out predominant criticisms. We then set out our network trespass theory in Part III, and argue that it is consistent with the CFAA's intended trespass foundations, it is narrow, and it will lead to better privacy and security outcomes in the long term. We also examine broader human rights implications of our account in Part IV.

II. *WHATS APP v. NSO GROUP*

Before addressing criticisms, it makes sense to briefly discuss the allegations and their context. The Complaint sets out a range of factual and legal allegations against NSO Group and centers on a security vulnerability in

45. Defendants' Motion for Summary Judgement at 2–8, WhatsApp, Inc. & Facebook, Inc. v. NSO Grp. Technologies Ltd. & Q Cyber Technologies Ltd., No. 3:19-cv-07123, 2015 WL 1033734, (N. D. Cal. Oct. 29, 2019).

46. *Id.* at 8–15.

47. Complaint, *supra* note 23, at 11–13; Greenberg, *supra* note 33 (quoting Riana Pfefferkor, cybersecurity expert at Stanford Law, noting the CFAA as the "main show" in the lawsuit).

the WhatsApp messaging service discovered in May 2019 and widely reported at the time[48] that exposed WhatsApp users to unauthorized tracking and surveillance. Facebook's security advisory described the vulnerability as one exploited through "remote code execution" via "specially crafted series of RTCP packets" sent, via WhatsApp's messaging network, to the phone numbers of targeted users.[49] Put in less technical terms, the attackers sent malicious code over the WhatsApp message service network that was specially designed to exploit a flaw in the network.[50] This malicious code, which could be delivered simply by virtue of a missed phone call without any interaction by victims, triggered the download of spyware onto targets' phones.[51] The spyware gave the attackers full access and control over victims' smartphones remotely, including access to messages that they normally could not access because of WhatsApp's end-to-end encryption as well as files, emails, call logs, text messages, photos, and videos—in short, everything.[52] The spyware, according to reports, bore all the hallmarks of NSO Group's Pegasus spyware tool.[53] After the lawsuit was filed, Citizen Lab issued a statement regarding research it had done linking NSO Group and the Pegasus spyware to the attack and identifying over one hundred cases of human rights defenders victimized globally, including civil society groups, activists, lawyers, and journalists located throughout the world.[54]

This is essentially what is alleged in the lawsuit, with a few additional technical insights as how the attack was carried out. First, the Complaint asserts that NSO Group ("the Defendants") created "various WhatsApp

48. Mehul Srivastava, *WhatsApp voice calls used to inject Israeli spyware on phones*, FIN. TIMES (May 13, 2019), https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab?; Julia Carrie Wong, *WhatsApp urges users to update app after discovering spyware vulnerability*, THE GUARDIAN (May 14, 2019), https://www.theguardian.com/technology/2019/may/13/whatsapp-urges-users-to-upgrade-after-discovering-spyware-vulnerability; Nick Hopkins & Stephanie Kirchgaessner, *WhatsApp sues Israeli firm, accusing it of hacking activists' phones*, THE GUARDIAN (Oct. 29, 2019), https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones.

49. *Security Advisory*, FACEBOOK (Aug. 13, 2019), https://www.facebook.com/security/advisories/cve-2019-3568; *The NSO WhatsApp Vulnerability—This is How It Happened*, CHECK POINT RES. (May 13, 2019), https://research.checkpoint.com/2019/the-nso-whatsapp-vulnerability-this-is-how-it-happened/.

50. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

51. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

52. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

53. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

54. *NSO Group / Q Cyber Technologies Over One Hundred New Abuse Cases*, CITIZEN LAB (Oct. 29, 2019), https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

accounts," "agreed" to the WhatsApp Terms of Service in doing so,[55] then "reverse-engineered" the WhatsApp app, and "developed a program to enable them to emulate legitimate WhatsApp network traffic."[56] This was done in order to surreptitiously "transmit malicious code—undetected—to Target Devices over WhatsApp servers."[57]

Second, the Defendants "routed and caused to be routed" the malicious code through WhatsApp's servers—including "Signaling Servers and Relay Servers—concealed within part of the normal network protocol."[58] They then used, without authorization, the Signaling Servers to transmit the "malicious code" to the Target Devices, bypassing restrictions on the Signaling Servers and concealing the malicious code in normal call traffic.[59] The malicious code was "injected" into the memory of Target Devices, and the Defendants later used Relay Servers to send encrypted packets also designed to "activate" the malicious code installed in the memory of Target Devices, triggering them to download spyware controlled by the Defendants.[60]

Third, the Complaint alleged the Defendants attempted to hack 1,400 different users worldwide in April and May 2019.[61] Based on these facts, the Complaint asserts multiple claims under the CFAA, including that the Defendants intentionally accessed without authorization a protected computer; knowingly, and with intent to defraud, accessed a protected computer without authorization contrary to sections 1030(a)(2)), 1030(a)(4), and 1030(b); as well as various claims of damages and loss.[62] We do not analyze each and every one of these claimed violations but focus on the central claims—whether the attackers either accessed without authorization or exceeded authorized access.

55. Complaint, *supra* note 23, at 7.

56. Complaint, *supra* note 23, at 8.

57. Complaint, *supra* note 23, at 8.

58. Complaint, *supra* note 23, at 8. The WhatsApp messaging network implements a version of the WebRTC, or Web Real Time Communications, protocol. Under WebRTC, "relay servers" are servers that facilitate communications between users on the network when direct peer-to-peer connections are not possible, while signaling servers sent information over the network to help to initialize connections between users via the relay servers. *See* Ivan Drnasin, Mislav Grgic & Gordan Gledec, *Exploring WebRTC Potential for DICOM File Sharing*, 33 J. DIGITAL IMAGING 697, 698 (2019); Sam Dutton, *Getting Started with WebRTC*, HTML5 ROCKS BLOG (Feb. 21, 2014), https://www.html5rocks.com/en/tutorials/webrtc/basics/.

59. Complaint, *supra* note 23, at 8.

60. Complaint, *supra* note 23, at 8–9.

61. Complaint, *supra* note 23, at 9.

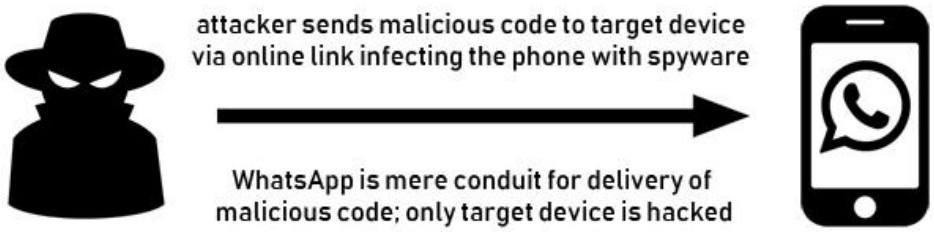
62. Complaint, *supra* note 23, at 10–11.

III. CRITICISMS AND POST-*VAN BUREN* PROBLEMS

The two most important criticisms concern the theoretical premises of the lawsuit itself. And both, in turn, have been strengthened by the Supreme Court's decision in *Van Buren*. First, the lawsuit, critics allege, relies primarily on terms of service violations as a theory of CFAA liability.[63] If so, then that *would* be a serious problem as it would be inconsistent with the "narrow reading" of the CFAA endorsed by the Supreme Court in *Van Buren*.[64] Second, the lawsuit deploys a "risky" or dangerously broad interpretation of the CFAA by alleging the Defendants are liable for unauthorized access simply because they allegedly used that network in ways WhatsApp did not authorize or approve; on this angle of view, only the targeted WhatsApp users are the victims, not WhatsApp.[65]

Each of these criticisms is based, to varying degrees, on a deeper theoretical understanding of the WhatsApp messaging network and the nature of the attack on WhatsApp users. This understanding or model of the attack is visualized in Figure 1, with an attacker focused on targeted users and WhatsApp merely a conduit for delivering the attacker's malicious code to the target.

Figure 1: Traditional Hack/Attacker Model[66]



On this traditional model or understanding of the attack, the real victims here are the end users: those WhatsApp users whose smartphones were

63. *See* Ekeland, *supra* note 31; Greenberg, *supra* note 33 (quoting Ekeland and Pfefferkor); Condliffe, *supra* note 30 (quoting Ekeland and Pfefferkor).

64. Kerr, *supra* note 11, at 1146.

65. Wolff, *supra* note 35; Ekeland, *supra* note 31 (arguing the Complaint reads as if there was "unauthorized access" because the Plaintiffs "didn't like the way their network was used," and insists that "if that's the standard for CFAA liability . . . then most of the internet is in trouble.").

66. The spy icon in this figure was created by Hopstarter and its production here is licensed under CC BY 4.0. The smartphone icon is public domain and not restricted by copyright (CC0 1.0).

infected by malicious code that caused their devices to download and install spyware giving control to third parties—clients and customers of NSO Group, as the Complaint alleges. On this view, WhatsApp, by contrast, was not hacked. It was simply a conduit for the attack—analogous to the open internet—but has no recourse under the CFAA. There are at least three "computer systems" on this understanding: the sending WhatsApp user device; the WhatsApp network; and the receiving WhatsApp user device. On this view, the users, not WhatsApp, are the proper plaintiffs in the action, as it is their information on their personal devices accessed without authorization. Putting this understanding in the terms used by the Supreme Court in *Van Buren*, the alleged attackers here, who had access to the WhatsApp network, did not obtain or alter information in "other areas" of the computer system in which they had access.[67] Rather, they entered an entirely different computer system—the smartphones of targeted users.

This theoretical approach, in our view, misunderstands the nature of the attack and how best to theorize it under the CFAA.

IV. UNDERSTANDING THE ATTACK AS A NETWORK TRESPASS

As noted in the previous Part, courts and commentators have been divided over the scope and application of the CFAA[68] with multiple different approaches employed in case law and scholarship.[69] More recently, however, leading scholars and experts like Orin Kerr, Josh Goldfoot, and Aditya Bamzai have advanced a "trespass" theory of the CFAA as a means to unify existing case law, theory, and approaches on point.[70] Indeed, successive House Reports through the 1980s, which led to the CFAA's enactment, described computer hacking, or unauthorized access to computer networks, as "trespassing" and described hackers to "trespassers."[71] A Senate Report that led to CFAA amendments in 1996 employed the same view, observing that the CFAA "criminalizes all computer trespass."[72] More recently, courts

67. Van Buren v. United States, 141 S. Ct. 1648, 1651–59, 1662 (2021); Kerr, *supra* note 10.

68. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562 (2010).

69. Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1445 (2016); Kelsey T. Patterson, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 499 (2013).

70. Kerr, *supra* note 11; Goldfoot & Bamzai, *supra* note 11; *see also* O'Connor, *supra* note 11.

71. Goldfoot & Bamzai, *supra* note 11, at 1482.

72. Goldfoot & Bamzai, *supra* note 11, at 1482; Kerr, *supra* note 11, at 1144 n.3.

have increasingly interpreted and applied the CFAA through a trespass framework[73] with the law's central "unauthorized access" concept interpreted as reflecting the right to exclude others from accessing property in traditional trespass law.[74] And now, the Supreme Court has largely vindicated this approach in *Van Buren*.[75]

A trespass framework also offers the best approach to theorize encrypted networks under the CFAA. But translating these largely settled physical trespass norms and requirements into computer and digital contexts—where they are largely unsettled—creates difficulties.[76] On this count, we agree with Kerr and others that a "code-based" standard offers the optimal means to operationalize trespass requirements in digital and computerized contexts.[77] That is, unauthorized access or exceeding authorized access is best understood under the CFAA as access to a computer that violates, breaks, by-passes, or circumvents a code-based restriction, barrier, or authentication gate. Put simply, the access barrier, restriction, or authentication gate violated by the trespasser on this interpretation is one implemented by the code, design, and architecture of the computer or the computer network accessed.[78] Indeed, based on *Van Buren*, it is likely the Supreme Court likewise favors a code-based approach to access restrictions, including in deciding if a user has exceeded authorized access to a computer network.[79]

Employing a code-based approach to exceeding authorized access under the CFAA, our network trespass theory is simple. The WhatsApp messaging network's central design feature is end-to-end encryption, which was incorporated in the messaging service to protect the privacy and security of user communications.[80] The WhatsApp messaging network's central design

73. Goldfoot & Bamzai, *supra* note 11, at 1482–83; Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1396 (2007).

74. Goldfoot & Bamzai, *supra* note 11, at 1478–79; Kerr, *supra* note 11, at 1144 n.3.

75. Kerr, *supra* note 10 (stating that the Supreme Court in *Van Buren* "settles that the CFAA is fundamentally a trespass statute").

76. Kerr, *supra* note 11, at 1147.

77. *See* Kerr, *supra* note 11, at 1147 (articulating an "authentication gate" standard as offering the best balance between open internet norms and the CFAA's trespass norms); Kerr, *supra* note 21, 1657–58 (advancing a "code-based restriction" interpretation of the CFAA's liability standard); *see also* Bellia, *supra* note 69; Patterson, *supra* note 69, at 528 ("[C]ourts should expressly adopt a code-based approach to [the CFAA's] interpretation.").

78. *See* Goldfoot & Bamzai, *supra* note 11, at 1487–88 (discussing code-based restrictions).

79. *See supra* note 12.

80. *Security*, WHATSAPP, https://www.whatsapp.com/security (last visited Oct. 1, 2020) [hereinafter *WhatsApp Security*]; *About End-to-End Encryption*, WHATSAPP, https://faq.whatsapp.com/en/general/28030015/?category=5245250 (last visited Oct. 1, 2020) [hereinafter *WhatsApp Faq*]; WHATSAPP ENCRYPTION OVERVIEW: TECHNICAL WHITE

feature is end-to-end encryption, which was incorporated in the messaging service to protect the privacy and security of user communications.[81] The attackers, alleged to be NSO Group, took steps—including spoofing WhatsApp client software, exploiting security vulnerabilities, and concealing and sending malicious code in normal network traffic via WhatsApp servers, thereby infecting WhatsApp user devices—in order to access user communications by circumventing the end-to-end encryption protecting them. In other words, the Defendants knew about a clear prohibition or code-restriction on access to user communications within the WhatsApp messaging network—the code-based end-to-end encryption—and violated that restriction by taking multiple steps to circumvent the encryption to access user communications, among other data. This is a trespass, on traditional trespass requirements, but not just on the users; but on the WhatsApp messaging network itself.

That sounds simple enough. But this network trespass theory involves two important but subtle legal and theoretical shifts in applying parts of the CFAA. First, we argue for a different theoretical understanding and scope of the "computer system" at issue here—WhatsApp's encrypted communications network. Rather than theorizing user devices—through which users interface with the network via a software client—as separate computer systems, we argue they ought to be treated as constitutive of the same network for the purposes of determining CFAA liability. Typically, we think of computer networks—like the internet—as simply a series of interconnected but separate computers.[82] This assumption actually underlies some of the central criticisms of the *WhatsApp v. NSO Group* lawsuit, which hold that the *real* victims of the hack are the users whose personal devices—separate computers from the WhatsApp network—were compromised and accessed. We argue this assumption makes sense for open networks like the internet but not encrypted networks like WhatsApp. Second, we argue that in order to understand when a code-based access barrier or authentication gate

PAPER (2020), https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=2&_nc_sid=2fbf2a&_nc_ohc=U4i2jUSaMEwAX-X1U2J&_nc_ht=scontent.whatsapp.net&oh=15593989c0626ebf40856b6468164a7e&oe=601F0119 [hereinafter WHATSAPP ENCRYPTION]; WHATSAPP, https://www.whatsapp.com (last visited Oct. 1, 2020) [hereinafter WHATSAPP WEBSITE].

81. *WhatsApp Security*, *supra* note 80; *WhatsApp Faq*, *supra* note 80; WHATSAPP ENCRYPTION, *supra* note 80; WHATSAPP WEBSITE, *supra* note 80.

82. MICROSOFT COMPUTER DICTIONARY 12 (4th ed. 1999) ("A group of computers and associated devices that are connected by communications facilities"). A DICTIONARY OF COMPUTING 5 (6th ed. 2008) ("the shared use of a series of interconnected computers, peripherals and terminals").

has been circumvented to trigger liability, the *intended function* of the code-based barrier in a computer system or network should be taken into account. Focusing on only how a code-based measure authenticates users can miss how attackers formulate sophisticated attacks that, rather than tricking or compromising the authentication gate itself, wholly circumvents it. Such "work around" attacks are common particularly with stronger forms of code-based access barriers that are harder to trick, compromise, or hack—like encryption. Instead, attackers find a way to work around the barrier. That is essentially what the attackers did here according to the alleged facts, and it should trigger CFAA liability.

A. THEORIZING THE SCOPE OF THE RELEVANT "COMPUTER SYSTEM"

Our first task is to theorize the proper scope and boundaries of the relevant "computer system" at issue.[83] Defining the scope, boundaries, and areas of the computer system at issue here—the WhatsApp encrypted network, as well as the information accessed therein—is critical because depending on whether the targeted users are part of the network or not will impact whether the attackers exceeded any authorized access by accessing "other areas" within a "computer system."[84] On this count, critics of the WhatsApp lawsuit argued the attackers were simply using the WhatsApp messaging network to target end-users[85] as if it was merely a conduit or staging ground for the attack. They also analogized WhatsApp to the open internet, a network over which the hack was staged but separate from the relevant computer system that was actually hacked—the targeted devices of users. As such, WhatsApp is not the victim, only targeted users. These are intuitive arguments because people access WhatsApp via their smartphones, and smartphones are themselves stand-alone personal computing devices. And we tend to think of computer networks as simply a series of connected but separate or individual computers with the internet being a key such example.[86]

This is important because, as alleged in the Complaint, the Defendants created accounts on the WhatsApp messaging network to carry out the

83. Mayer, *supra* note 17, at 1646.

84. Atlas et al., *supra* note 10 (noting that "[t]he key inquiry under the CFAA" involves determining whether an individual had authorized access to the "areas of a computer system at issue"); Cunningham, Grant & Hoofnagle, *supra* note 19.

85. Wolff, *supra* note 35; Ekeland, *supra* note 31 (arguing the Complaint reads as if there was "unauthorized access" because the Plaintiffs "didn't like the way their network was used," and insists that "if that's the standard for CFAA liability . . . then most of the internet is in trouble").

86. *See supra* note 82 and accompanying text.

attack.[87] So, it is likely the Defendants had "authorized access" to the WhatsApp network, at least initially,[88] and thus a key issue for CFAA liability is whether they "exceeded authorized access."[89] That phrase is expressly defined in the statute to "access a computer with authorization" and to use that access to "obtain or alter information" that "in the computer" that the attacker is "not entitled so to obtain or alter." That language—"in the computer"—means that exceeding authorized access involves hacking *in the computer system itself* and not using it as a staging ground or conduit for attacks on other computers, as critics argue. In other words, if we accept that WhatsApp user devices are separate computers from the WhatsApp network, any information obtained or altered on them are not "in the computer" or WhatsApp network, and thus attackers would not have exceeded their access and would not be liable.

Nevertheless, we believe a proper legal and technical understanding of the WhatsApp network would approach user devices as a key part of the network itself, and not separate. In determining the scope of the relevant computer system or service and the information therein for CFAA purposes, we agree with Jonathan Mayer that an "objective" approach that takes into account the perceptions of ordinary users is preferable.[90] However, we would also include two other factors in making this determination: the technical realities of the computer system, service, and information and the nature of the hack itself. In other words, what was the information the attackers were targeting and what was their methodology? Applying this approach, WhatsApp users and their devices should be theorized as central parts of the WhatsApp network, not separate computer systems.

First, an ordinary user would not only perceive the WhatsApp messaging network as one system as a whole—as our analysis has argues—but also that an individual account on that system constitutes a "distinct set of information." This means, accessing other user accounts and their information would almost surely be understood by ordinary users as accessing "other areas" on the computer system to which their own authorized access would not extend. No reasonably or ordinary user would

87. Complaint, *supra* note 23, at 7–8.

88. Mayer, *supra* note 17, at 1646. Of course, it could also be argued that if they had created accounts *only* for the purpose of carrying out the attack, there was no permission or authorization at any stage.

89. 18 U.S.C. § 1030(a)(2)(C) (2018) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section."); 18 U.S.C. § 1030(e)(6).

90. *See* Mayer, *supra* note 17, at 1653.

believe they would have access to the "information" of other users, like private messaging, data, media, files, and anything else shared via private chats. This is especially so given that WhatsApp promotes its end-to-end encryption as a central feature of the network that, as noted earlier, protects user messages, files, and information from other users, third parties, and from even WhatsApp itself. On this view, encryption is a clear code-based restriction on access to other user's "information"—that is, communications within that network.[91]

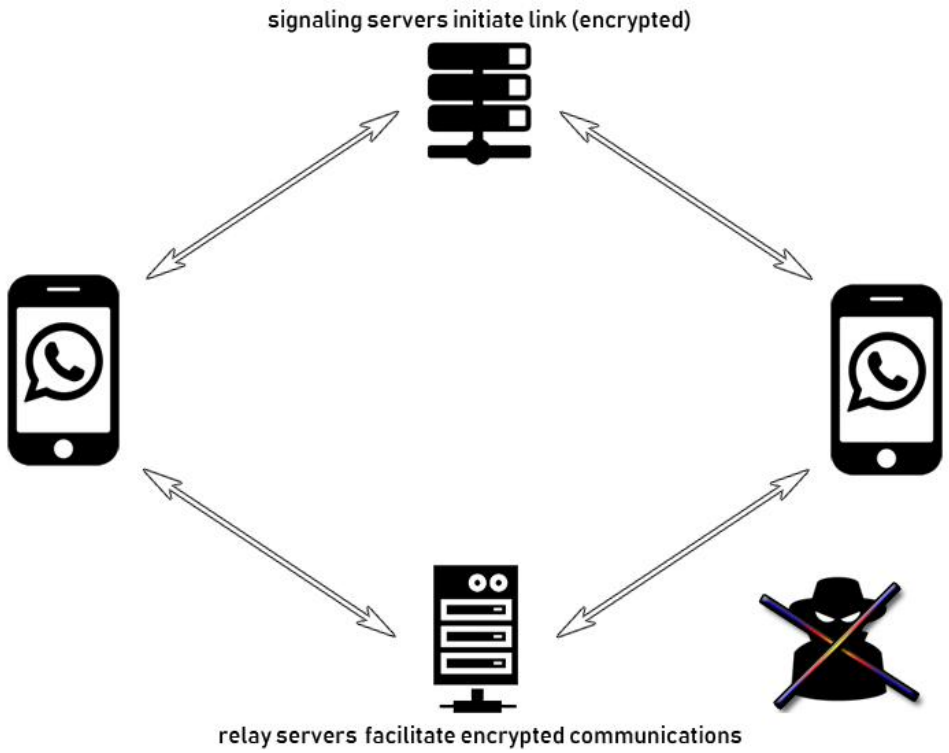
Second, the technical realities of the WhatsApp messaging network confirm these ordinary user perceptions. In the WhatsApp network, users—who interface via smartphone devices running the WhatsApp client—are not peripheral or separate from the system, but core to the functions of the network itself. This is clear from a visualization of the network itself in Figure 2.[92]

Figure 2: The End-to-End Encrypted WhatsApp Network[93] —The WhatsApp messaging network protects communications from third-party surveillance through end-to-end encryption.

91. *Id.*

92. WHATSAPP ENCRYPTION, *supra* note 80, at 3, 11; *WhatsApp Security*, *supra* note 80.

93. Both Figure 2 and Figure 3 were created drawing on alleged facts and details in the Complaint as well as on other related commentary, research, and documentation. *See supra* notes 3–33. The network server icons used in this figure are licensed under CC BY 4.0 by SVG Repo. The spy icon in this figure was created by Hopstarter and is licensed under CC BY 4.0. The smartphone icon is public domain and not restricted by copyright (CC0 1.0).



Visualized in Figure 2, the notion of the WhatsApp messaging service *as a network* is clear. Included in the network are all WhatsApp users; their client applications (smartphone app or web-based); and a series of server nodes (Signal and Relay Servers) that initiate, coordinate, and facilitate all communications and data across the network. When a user drafts and sends a message on their WhatsApp client, it is immediately encrypted by the sender's client. This initiating or sending user's client then sends a request to the Signaling Servers to initiate an encrypted link between the sending user and the recipient user. Relay Servers also facilitate encrypted communication data transmissions between users, especially where obstacles such as firewalls exist. The Recipient's WhatsApp client receives encrypted messages, which are then decrypted using both a public and private key. What is also clear from this visualization is that users are not peripheral to the messaging network, but core to its central function—communications. At the same time, the technical reality is consistent with ordinary user perceptions—each user account, client, or device, though part of the overall computer network or system, are nevertheless distinct elements of that network. Due to end-to-end encryption, users do not have access to the encrypted messages of any other users.

Furthermore, analogizing the WhatsApp messaging network to the open internet is incorrect, both legally and technically. The WhatsApp messaging network is not the open internet nor is it an open network or web service. First, the central design feature of WhatsApp's messaging network is end-to-end encryption, a code-based barrier that encloses the entire network from outsiders seeking to intercept user communications. The internet's fundamental architecture lacks this design feature—it is open and general.[94] This open and flexible architecture made communications and connectivity easier, but also made surveillance and eaves-dropping far easier as well.[95] Second, unlike the open internet or web, to use Kerr's terms, not all visitors "get service."[96] To access the network, a user must first create an account, agree to the TOS, and then download and install onto their device the authorized WhatsApp smartphone client apps or log into the authorized WhatsApp web-based client.[97] Finally, once accessing the WhatsApp messaging network, all communications data between users are routed through WhatsApp servers in accordance with WhatsApp-specific protocols.

Third, the nature of the attack also demonstrates the same. When an insider threat or "inside hacker"—as the Defendants are alleged here to be—seeks to access or misappropriate the "information" of other users in the network—like the messages, files, media, and other information shared on the WhatsApp network and stored on their user devices— it is not an attack on separate individual computer systems, but an attack or trespass on the WhatsApp network itself. Here, the attackers sought access to the WhatsApp network by creating accounts. They then reverse engineered the Whats App client and connected it to the network. They then sent malicious code over the network to targeted WhatsApp users, which infected their user devices also via the network. This is because those user devices, loaded with the WhatsApp client, are essential for users to interface with the network. From the perspective of the attackers and their target, the boundaries of the WhatsApp network include WhatsApp users and the means by which they interface with the network—individual WhatsApp client accounts on their smartphone devices. Here, while WhatsApp users have separate accounts, they constitute distinct divisions, units, or "areas" within the network but are not separate computer systems. So, the alleged attack did not involve accessing the separate computers of targeted user, with WhatsApp the

94. *See* Kerr, *supra* note 11, at 1162–63.

95. *Communicating with Others*, ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE GUIDE (June 9, 2020), https://ssd.eff.org/en/module/communicating-others.

96. *See* Kerr, *supra* note 11, at 1162.

97. Complaint, *supra* note 23, at 4.

conduit or staging ground for the attack, but instead involved an accessing information in "other areas" within the WhatsApp messaging network itself—on the accounts of other users.

Lastly, the WhatsApp messaging network clearly falls within the definition of "computers" and "protected computers" in the CFAA.[98] Again, critics of *WhatsApp v. NSO Group* argue that the proper plaintiffs in the lawsuit should be the targeted users whose smartphones were compromised, not WhatsApp itself.[99] But these criticisms ignore the fact that these definitions are sweeping in scope and almost certainly cover the WhatsApp messaging network itself, beyond simply its constituent servers and the connected devices of users. Indeed, the broad wording of the "computer" definition includes any "communications facility directly related to or operating in conjunction with" computers like the smartphones and computers used by WhatsApp users.[100] Certainly, the WhatsApp messaging network qualifies as such a "facility" and courts have agreed. The Ninth Circuit in *Nosal (II)* noted that "protected computers" include computer networks, databases, and radio communications networks.[101]

But beyond the broad definitions, courts have also theorized networks that consisted of individual computers and computerized components under the CFAA as a whole or single system, rather than dividing up the network among those constituent devices or computers for the purposes of analysis. In *Mitra*, for example, the Seventh Circuit upheld the accused's conviction under the CFAA for intentionally damaging a radio communications network called "SmartNet II," which was designed by Motorola and used by police, fire, ambulance, and other agencies for emergency communication.[102] Justice Easterbrook, writing for the court, found that SmartNet radio communications network was "as a whole" a "protected computer."[103] This was despite the fact that the SmartNet had countless computerized constituent elements, including computer hardware and software components, multiple "roaming units," and a "trunking system" to utilize

98. *See* 18 U.S.C. § 1030(e)(1); *see, e.g.*, United States v. Nosal (*Nosal II*), 844 F.3d 1024, 1050 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 314 (2017) (noting "protected computers" include "effectively all computers with Internet access . . . nearly all desktops, laptops, servers, smartphones . . . .").

99. *See supra* note **Error! Bookmark not defined.**.

100. 18 U.S.C. § 1030(e)(1); *see Nosal II*, 844 F.3d at 1050.

101. *Nosal II*, 844 F.3d at 1032 n.2, n.3.

102. United States v. Mitra, 405 F.3d 492 (7th Cir. 2005) (recognizing that a radio system is a computer).

103. *Id.* at 494.

broadcast frequencies efficiently.[104] This makes sense given the three factors employed above. Ordinary users would certainly perceive SmartNet as best understood as a communications network as a whole, rather than individualized computer components included in the network to ensure it operates properly. The technical realities also support this conclusion, with the various computerized components all included in the network to facilitate core functions of the overall network. Lastly, the nature of the attack also shows supports this conclusion—Mitra did not seek to use the network to hack other computer system, but his aim was to target individual parts of the network in order to disrupt it as a whole. Similarly, the WhatsApp messaging network—and similarly designed internet and social media communications platforms—should likewise be theorized "as a whole," with different computer components constituting particular areas within the network.

All of these points support the same conclusion—users, and the accounts and devices they use to interface with the WhatsApp network, are best understood as distinct "areas" within the broader computer system itself, the WhatsApp network. And the design of the network means that each user has an individual account tied to a smartphone that cannot be accessed by other users, with end-to-end encryption as a layer of protection to ensure each user's messages and information are private and not accessible by other users, third parties, or WhatsApp network operators. As such, any existing WhatsApp user that access information in these "other areas"—other user accounts—does so without authorization.

B. CIRCUMVENTING THE CENTRAL CODE-BASED ACCESS BARRIER

As noted earlier, the Defendants had "authorized access" to the WhatsApp network, at least initially.[105] So, the central issue is whether the Defendants *exceeded* that authorized access in carrying out the attack. The meaning of "exceeds authorized access" in the CFAA has been contentious, but now it is much clearer thanks to *Van Buren*. Now, a user "exceeds" authorized access if they bypass or circumvent an access barrier or gate in order to access or alter information in "other areas" "within a [computer] system" that they never had permission or authorization to access initially.[106] We have already argued that the relevant scope of the computer system in question is the WhatsApp network as a whole, which includes users—who interface with the network via their individual WhatsApp account and WhatsApp clients on their smartphone devices. We have also argued that

104. *Id.* at 493–94.

105. *See supra* note 88 and accompanying text.

106. KOSSEFF, *supra* note 7, at 176–80; Mayer, *supra* note 17, at 1657–58.

those user accounts are also distinct "areas" within the network, separated by the general architectural design of the network and end-to-end encryption. As such, on the alleged facts, it is clear that the Defendants in ultimately accessing the "information" in other WhatsApp user accounts—messages, files, data, etc.—and have thus accessed an "other area" within the WhatsApp network. The remaining question, then, is whether a code-based access barrier was bypassed or circumvented in order to access these information.

But as with the scope of the relevant computer system, theorizing the scope and function of the code-based access barrier at issue, and how it was circumvented, also requires subtle legal and theoretical shift. Here, we approach the code-based access barrier—end-to-end encryption—not as simply an authentication gate that the attackers have tricked, compromised, or otherwise passed through. Rather, we focus on how the attackers circumvented a broader intended function in the WhatsApp network—protecting the privacy and security of communications and other information shared on the network.

1. The Access Circumvented a Code-Based Access Barrier

The Defendants' alleged hack here violated a clear and express "code-based" prohibition on access built into the WhatsApp messaging network end-to-end encryption.[107] Code-based limitations are attempts to enforce an owner's intent to limit authorization through the use of software, hardware, or other technical related measures.[108] Such restrictions are important because they define not only the limits of access but also communicate the owner's intent to limit access.[109] End-to-end encryption plays this role in WhatsApp. This code-based restriction or prohibition is "express[ed]" both as a feature highlighted and communicated by WhatsApp, but also in the architecture itself. In fact, it is a central technical WhatsApp feature, ensuring messages sent by users are protected by an end-to-end encryption protocol—where each message is encrypted with both a public and private key before being sent so that only the recipient can decrypt and read the messages. This is all apparent in Figure 2, discussed earlier.

But it is not just messages that are encrypted in this network. Rather, the entire communications network is protected in a layer of end-to-end encryption. Meaning every step and function in the network—from messaging session initiation, to receiving session setup, to messaging

107. Goldfoot & Bamzai, *supra* note 11, at 1487; *see* Kerr, *supra* note 11, at 1147.
108. Goldfoot & Bamzai, *supra* note 11, at 1487.
109. *Id.* at 1490.

exchange, to transmitting media and other attachments, to group messages, to voice and video call setup, to status and location updates—is protected by end-to-end encryption.[110] Thus, if a third party could intercept a message before it arrived with the recipient, they would not be able to decrypt without the recipient's private key. This code-based restriction, which protects the privacy and security of all WhatsApp user messages, applies both to insiders and outsiders. That is, the encryption ensures only the intended recipient can decrypt and read messages—not other users, nor hackers or attackers outside the network, nor even WhatsApp itself.[111]As earlier noted, encryption has long been recognized as a "code-based" restriction on access under the CFAA.[112] The difference here is that it is not a single file or transfer that is encrypted to prevent access; rather, the entire WhatsApp messaging network is enclosed by end-to-end encryption—a clear and express prohibition on access to communications within the network.

2. The Attackers Knew of the Code-Based Access Barrier

The Defendants, on these alleged facts, knew of the code-based restriction—the end-to-end encryption. Beyond being a central technical and architectural feature of WhatsApp's messaging network, encryption is highlighted and persistently advertised on the WhatsApp website as a key feature, including in a technical white paper available on the site.[113] In fact, the entire hack, visualized in Figure 3, evinces a sophisticated understanding of the WhatsApp network and its encryption protocol.

Figure 3: The Alleged WhatsApp Messaging Network Hack — Multiple steps and involving multiple provides unauthorized access and exploitation of every aspect of WhatsApp's messaging network.

110. *See* WHATSAPP ENCRYPTION, *supra* note 80, at 11.

111. *See id.*

112. *See* Kerr, *supra* note 21, at 1666 (analyzing a scenario involving an encrypted internet connection as a "code-based" restriction under the CFAA); *see also* Clark S. Splichal, *Recent Development: Craigslist and the CFAA: The Untold Story*, 67 FLA. L. REV. 1845, 1856 (2015) (noting encryption is a "conventional" technological or code-based "barrier" like passwords).

113. *See* WHATSAPP WEBSITE, *supra* note 80; *WhatsApp Security*, *supra* note 80; *WhatsApp Faq*, *supra* note 80; WHATSAPP ENCRYPTION, *supra* note 80.

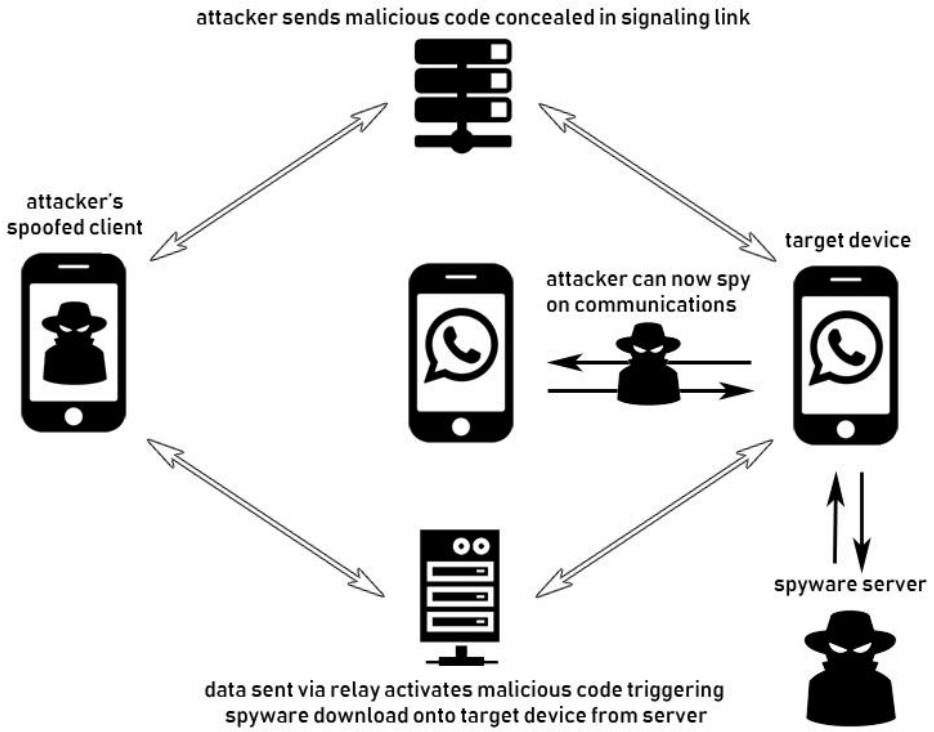


Figure 3 helps illustrate that instead of attempting to break the encryption from the outside, the attackers focused on circumventing it by targeting vulnerable points in the WhatsApp messaging network—WhatsApp clients, network protocols, server nodes, and target devices—to get around the encryption protection and obtain unauthorized access to communications within the network. The Defendants, the Complaint alleges, first created "various WhatsApp accounts" and then "reverse-engineered" the WhatsApp user app in order to develop a spoofed WhatsApp client program ("spoofed client" in Figure 3).[114] This spoofed WhatsApp client was able to emulate "legitimate" WhatsApp messaging network traffic, thus enabling them to send "malicious code"—undetected—via the WhatsApp messaging network.[115] The Defendants then transmitted malicious code via the WhatsApp messaging network, specifically the Signaling Servers, to the targeted user ("target device" in Figure 3).[116] This instance of malicious code—which could be delivered simply by a missed WhatsApp call on the target device—was specially designed to exploit a flaw in WhatsApp's end-to-

114. Complaint, *supra* note 23, at 7–8.
115. Complaint, *supra* note 23, at 8.
116. Complaint, *supra* note 23, at 8.

end encryption protocol, allowing it to install in the memory of the target device.[117] An additional instance of malicious code was then transmitted by the Defendants, this time via the WhatsApp Relay Servers, which triggered the download of spyware onto the target device from a remote server controlled by the Defendants.[118] The spyware, once installed, could be controlled remotely by the Defendants and provided them access to all data on the target device, including access to WhatsApp messages, call logs, and other data and information shared on the WhatsApp network that was previously inaccessible because of encryption.[119] The alleged spyware in question—Pegasus—is specifically designed to circumvent end-to-end encrypted communications on services like WhatsApp, as once it is downloaded and installed on a target device, it is designed to intercept messages before they are encrypted on the client application and sent across the network or after the client applications decrypts.[120]

The Defendants carried a multi-step sophisticated hack, specifically designed to exploit unique aspects and vulnerabilities in the WhatsApp messaging network to circumvent a central code-based restriction built into the WhatsApp messaging network as a whole: end-to-end encryption protection for user messages. Like the hack in *Barrington* found to violate the CFAA, this hacking scheme also involved "multiple, repetitive and coordinated steps to deceive and exploit" WhatsApp's encryption-protected network.[121] Also like *Barrington*, it involved "repetitive and coordinated activities by numerous individuals" who used "sophisticated technology" to carry out and "conceal" the scheme.[122] This kind of sophisticated attack that led to access and entry to user devices is precisely the kind of malicious activities the CFAA should deter and police.

Indeed, the visualizations in Figures 2 and 3 also help illustrate how WhatsApp messaging service operates like a system or network enclosed by encryption protection from end-to-end, and how the attack was an attack or

117. Checkpoint Research, *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

118. Checkpoint Research, *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48; Complaint, *supra* note 23, at 7.

119. *See* Checkpoint Research, *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

120. *See* Complaint, *supra* note 23, at 6; Lorenzo Franchesci-Bicchierai & Joseph Cox, *The DEA Didn't Buy Malware From Israel's Controversial NSO Group Because It Was Too Expensive*, VICE: MOTHERBOARD (Sept. 11, 2019), https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo; *Protecting our users from a video calling cyber attack*, WHATSAPP (Oct. 29, 2019), https://faq.whatsapp.com/general/security-and-privacy/protecting-our-users-from-a-video-calling-cyber-attack/?lang=en (explaining the NSO Group's attack).

121. United States v. Barrington, 648 F.3d 1178, 1199 (11th Cir. 2011).

122. *Id.*

unauthorized trespass on that network as a whole. And this encryption, which encloses the network, defines unauthorized access and any access that exceeds authorized access. In this sense, it was like the attack on the radio communications network in *Mitra*, which compromised the integrity and operations of the network. WhatsApp is not just users messaging across the internet; it is a sophisticated messaging network with nodes, servers, and users—like a circuit—and protected by encryption throughout. The Defendants exploited multiple vulnerabilities in various parts of the network—Signaling Servers, Relay Servers, user client apps, and user devices, among others—to go around it and target the weaker end-points—the unencrypted user devices.

If this theory and the facts underlying it are proven at trial, assuming the case proceeds that far, they will support multiple CFAA claims. They clearly demonstrate not only that the Defendants knew about the end-to-end encryption in the WhatsApp messaging network but intentionally circumvented it to access information in "other areas" in the "computer system"—the messages, files, media, and shared information of other WhatsApp users—to which their initial authorized access did not entitle them to access.[123] This was "information" they were not entitled to access and which was "in the computer," that is, in the WhatsApp network itself. As such, the Defendants would have "exceeded authorized access" to the WhatsApp messaging network contrary to section 1030(a)(2)(C).[124] On the CFAA's broad definitions of "damage," this will have certainly "damaged" the network by impairing its integrity.[125] These actions would almost certainly caused a "loss" to one or more persons (sections 1030(e)(11) and 1030(c)(4)(A)(i)(I)) and caused "damage" by impairing the integrity of the WhatsApp network (section 1030(e)(8)) by undermining its end-to-end encryption protections.

V. A NETWORK TRESPASS THEORY OF LIABILITY

We have argued that the alleged attack on WhatsApp's encrypted messaging network is best understood using what we call a network trespass theory of liability. This theory holds that accessing a network and using it to hack or stage an attack on users of that network—like obtaining unauthorized access to their personal computing devices by circumventing end-to-end encryption—should be treated as trespass not just on the

123. 18 U.S.C. § 1030(a)(2)(C); *id.* § 1030(e)(6).

124. 18 U.S.C. § 1030(a)(2)(C); *id.* § 1030(e)(6).

125. 18 U.S.C. § 1030(e)(8) ("[T]he term 'damage' means 'any impairment to the integrity or availability of data, a program, a system, or information.' "); *id.* § 1030(e)(6).

individual devices of the targeted users, but on the network itself, and it should thus attract liability under the CFAA.

The theory is consistent with the narrow reading of the CFAA endorsed in *Van Buren* and, applied to the alleged facts of *WhatsApp v. NSO Group*, offers a full answer to criticisms. Critics argued that the *WhatsApp* lawsuit relies too heavily on breach of the terms of service as a foundation for its claims under the CFAA.[126] And, to be clear, the Complaint does cite WhatsApp's Terms of Service and alleges that the Defendants accepted those terms.[127] Our network trespass theory of liability, however, focuses on how the Defendants circumvented code-based restrictions, avoids the problems critics raise, and is entirely consistent with a narrow interpretation of the CFAA, endorsed by the Supreme Court in *Van Buren*. To be clear, our network trespass theory does offer a new and novel approach to theorizing the "boundaries" of the "relevant computer system" and the "information and services with that system" in the CFAA analysis.[128] But this, as we have argued, is a better legal, theoretical, and technical understanding of the WhatsApp network.

A. THE CFAA'S POLICY AIMS

Why should this theory be applied here and beyond? First, imposing liability here, based on our network trespass theory, would advance the underlying policy aims of the CFAA. The statute was enacted in response to concerns about the growing threat hackers posed to computers and their security, both insiders and outsiders.[129] The sophisticated multi-stage hack carried out on the WhatsApp messaging network—to circumvent its end-to-end encryption protection of user communications—is precisely the kind of hack the CFAA was intended to cover. When applying the "intended function test" from the famous *Morris* worm case, for instance, the allegations show the Defendants clearly did not use the WhatsApp network as intended: not for messaging, but to circumvent encryption in order to access the messages of other users without authorization.[130]

Additionally, the statute, when passed, aimed not only to protect the security and integrity of computers and computer networks from hackers and

126. *See* Ekeland, *supra* note 31; Greenberg, *supra* note 33 (quoting Ekeland and Pfefferkor); Condliffe, *supra* note 30 (quoting Ekeland and Pfefferkor).

127. Complaint, *supra* note 23, at 4, 7.

128. Mayer, *supra* note 17, at 1646.

129. Winn, *supra* note 73, at 1402–03; Goldfoot & Bamzai, *supra* note 11, at 1481–82.

130. *See* United States v. Morris, 928 F.2d 504 (2d Cir. 1991); Kerr, *supra* note 21, at 1631–32.

unauthorized intrusion—hence the incorporation of legal concepts from trespass law—but also to protect information and data contained on computers.[131] Encryption is an essential technological tool for such protection. Today, it is considered a "fundamental architectural safeguard" that permeates both law and private-sector cybersecurity frameworks.[132] And for the Financial Industry Regulatory Authority (FINRA), encryption is a "critically important" tool in a firm's cybersecurity "arsenal."[133] Thus, as a long-recognized "code-base" restriction on access that is now also "essential" to ensuring security and privacy in new forms of electronic communications systems,[134] imposing liability here is fully consistent with the CFAA's aims.

B. BETTER PRIVACY AND SECURITY OUTCOMES

Though the original CFAA statute did not highlight privacy concerns, subsequent amendments, particularly in 1996, made privacy concerns clear.[135] Concerns about protecting privacy in information to restore public faith in computer security can be found throughout legislative debates about the amendments.[136] Pursuant to these aims, enforcement and liability here would also lead to better privacy and security outcomes in the long term.

First, it offers an additional legal lever to deter and police insider threats under the CFAA. Cybercriminals, hackers, and other malicious actors have long used the computers, networks, and servers of others as staging grounds, mediums, or intermediaries to carry out attacks, hacking, and other illegal and disruptive activities online.[137] Such cases have raised the issue, also long

131. Winn, *supra* note 73, at 1404; Goldfoot & Bamzai, *supra* note 11, at 1481–82.

132. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1175 (2019).

133. *Id.* at 1190.

134. Tole Sutikno, Lina Handayani, Deris Stiawan, Munawar Agus Riyadi & Imam Much Ibnu Subroto, *WhatsApp, viber and telegram: Which is the best for instant messaging?*, 6 INT'L J. ELECTRICAL & COMPUTER ENGINEERING 909, 911 (2016).

135. Winn, *supra* note 73, at 1404–05; Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 330–31 (2004).

136. *See* Winn, *supra* note 73, at 1404–05; *see also* Galbraith, *supra* note 135, at 330–31.

137. In fact, one of the first hacking cases prosecuted under the CFAA was the *Morris* case. *See* United States v. Morris, 928 F.2d 504 (2d Cir. 1991). Edward Morris, then a Cornell graduate student, was prosecuted for damage caused by his computer worm, which infected computers and spread around the world via the internet. To launch his worm, Morris hacked into a computer at Massachusetts Institute of Technology (MIT) to conceal its origins. It did not work. *See The Morris Worm*, FBI NEWS STORY (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218; *see also* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure: A Duty of Care in*

debated, as to how the law should deal with intermediaries whose platforms are used and abused by hackers and malicious actors for such illicit activities,[138] including what recourse or protections such intermediaries might have under CFAA.[139] This issue has taken on even greater urgency in a world where popular social media and communications platforms—like Facebook, Twitter, and WhatsApp—are now ubiquitous, as these platforms typically have hundreds of millions, even billions, of users—a target rich environment for malicious actors—and are generally accessible to anyone with an internet connection.[140] This has created a range of new "insider" threats and risks, as users that already have authorized access to a platform or network—hence an insider—can use that access to target other users, misappropriate data and

Cyberspace, 32 N.M. L. REV. 11, 11–14 (2002) (detailing the story of "Mafiaboy," a 15-year-old "script kiddie" living with his parents in a Montreal suburb, who took down several major websites in February 2000 with a distributed denial of service (DDoS) attack, which often made possible by a network of infected third party intermediaries or "zombie" computers and servers); Helen Nissenbaum, *Where Computer Security Meets National Security*, *in* CYBERCRIME DIGITAL COPS IN A NETWORKED ENVIRONMENT 63 (Jack Balkin, James Grimmelmann, Eddan Katz, Nimrod Kozlovski, Shlomit Wagman & Tal Zarsky eds., 2006) (noting use of networked computers as staging grounds or mediums for online attacks and other disruptive activities as a key category of cybersecurity threats).

138. *See, e.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 29, 53–54 (2000) (arguing for nuisance law principles to apply in the internet context); Adam Mossoff, *Spam-Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 647–48 (2004) (similar); Henderson & Yarbrough, *supra* note 137, at 16–18 (exploring both the duty and standard of care, on a negligence law standard, involved in protecting a person's own computer against becoming a staging ground for attacks); T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 551–54 (2010) (arguing owners of infected computers in "botnet" or 'zombie" networks—often used in DDoS and similar attacks—should be held liable to DDoS victims under a negligence theory).

139. *See, e.g.*, Laura Bernescu, *When is a Hack not a Hack: Addressing the CFAA's Applicability to the Internet Service Context*, 2013 U. CHI. LEGAL F. 633 (2013) (considering CFAA's application to online service providers); *see generally* Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 168–74 (2018) (analyzing the CFAA's application to the Internet of Things and similar common intermediaries for forms of online attacks); Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229 (2014) (arguing that existing legal options are insufficient and proposing that the CFAA be amended to allow for innocent intermediaries of hacking and other cybercrimes to "hack back," that is, hack into the computer systems and servers of perpetrators and other third parties to deter attacks or assist in attribution); Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL'Y REV. 205 (2018).

140. *See* Margetts, *supra* note 15, at 107–08.

information, or carry out attacks or other illicit activities against targets elsewhere online.[141]

However, the Supreme Court in *Van Buren*, as earlier noted, significantly narrowed CFAA scope in deterring and policing such insider threats by finding there is no criminal or civil liability under the CFAA for improper use of that system or information—like using a platform as a staging ground to hack, target users, or engage in other illegal activities. Now, the only way an insider threat can exceed their authorized access under the CFAA is when they access files, data, or information in other areas "in the computer" to which they had no access to begin with.[142] Our approach offers a new theory of network trespass liability to allow platforms and networks like WhatsApp to legally defend themselves from insider threats.

Indeed, applying CFAA restrictions to prohibit and punish this sophisticated hack would help deter hackers and other bad actors—such as firms creating, selling, and distributing spyware and malware—from similarly attacking and circumventing similar encryption protocols in the future. Indeed, it has been recently argued that a negative consequence of the WhatsApp lawsuit, if such lawsuits become more common, is it may cause the "market in cyber vulnerabilities" to "dry up," limiting the government's capacity for legal hacking as there be fewer "cyber vulnerabilities" for it to purchase or acquire from private actors.[143] Having fewer cyber vulnerabilities being bought, traded, and shared would be a positive outcome for privacy, security, and human rights in the long run. As Justice Fletcher wrote in *Bernstein v. United States*, the availability and use of encryption by citizens offers the opportunity to "reclaim some portion of the privacy we have lost" through increasing electronic communications.[144] By providing protection for encryption protocols in messaging networks like those WhatsApp employed and in deterring exploitation of those systems, the CFAA can help promote such privacy aims.

It would also, in turn, encourage more companies and social media platforms to employ end-to-end encryption to ensure the privacy and security of users. Privacy law scholar William McGeveran, for instance, recently argued for a "duty of data security" that includes a mandatory duty to use encryption in certain circumstances.[145] One such instance might

141. *See supra* note 15; LUCAS WRIGHT, *supra* note 14, at 40. As mentioned, "insiders" commit most cybercrime. *See* Mayer, *supra* note 14, at 1493.

142. 18 U.S.C. § 1030(e)(6).

143. Rozenshtein, *supra* note 40; McGeveran, *supra* note 132, at 1191.

144. Bernstein v. United States, 176 F.3d 1132, 1146 (9th Cir. 1999).

145. McGeveran, *supra* note 132, at 1190.

include services or platforms comparable to WhatsApp where data is constantly "in transit"—like being transmitted between servers or users on a messaging network.[146] Beyond the technical safeguards encryption provides, the law could also provide an additional remedy when encryption is attacked, hacked, circumvented, or broken through sophisticated security vulnerability exploits or malicious code and programs designed to extensively invade the privacy of targeted users.

However, beyond outsider threats and attackers, it may be argued that this approach creates liability risks for existing users—network insiders—who use platforms like Facebook or WhatsApp contrary to how they were intended, like using "knock off" versions of smartphone applications.[147] These concerns are misplaced. First, on our network trespass theory, such activities—like using a knock off version of WhatsApp on the WhatsApp network—would not "exceed authorized access" as they would not involve circumventing a code-based restriction to access "information"—encrypted communications—of other user accounts on the system, as the Defendants have done here. Again, to attract liability for "exceeding" authorized access on a narrow interpretation of the CFAA involves circumventing code-based restrictions on access to services or information within the system that the user did not have access to initially. A "knock off" app that is only restricted by TOS and not any code-based or technological barrier would not attract liability. Second, these concerns also ignore *mens rea*, or intentions, a "critical" component of CFAA analysis.[148] The CFAA was enacted to address "serious computer break-ins,"[149] and such activities on the network simply do not qualify. If, however, creators of a knock-off app did so with the intent to exploit vulnerabilities in a network to surreptitiously access encrypted communications of other users—and did so—then this would be an *intent* and *conduct* that could lead to CFAA. Users taking advantage of "knock off" apps with different basic features to communicate legitimately with other users would not. By contrast, the Defendants alleged attack on the WhatsApp network, which circumvented encryption barriers, is clearly an intentional and "serious computer break-in"[150] in terms of the network.

146. McGeveran, *supra* note 132, at 1191.

147. *See* Yomi Kazeem, *WhatsApp is so popular in Africa, even knock-off versions are used more often than Facebook*, QUARTZ AFRICA (Mar. 5, 2020), https://qz.com/africa/1804859/fake-whatsapp-app-more-popular-than-facebook-instagram-in-africa/.

148. *See* Kerr, *supra* note 11, at 1180.

149. Jamie Williams, *Automation Is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. SCI. & TECH. 416, 437–41 (2018).

150. *See id.*

C. CORPORATE ACCOUNTABILITY FOR HUMAN RIGHTS VIOLATIONS

There is a broader international human rights context to the WhatsApp lawsuit, providing a good reason to support it beyond the legal or technical aspects of its claims. Though the lawsuit only asserts claims under U.S. laws like the CFAA, its international dimensions are clear. For instance, the Citizen Lab, as earlier noted, identified at least one hundred cases of human rights defenders victimized by the attack globally, including activists, dissidents, lawyers, and journalists throughout the world.[151] And WhatsApp CEO Will Cathcart cited privacy as a "fundamental right" and argued, "technology companies must deepen our cooperation to protect and promote human rights."[152]

But the human rights concerns raised by transnational private sector technology companies like NSO Group go far beyond one single company. The Citizen Lab, for example, has documented numerous instances of private sector companies operating internationally and contributing to human rights abuses.[153] Filtering technology developed by Canadian company Netsweeper, for instance, has been used by governments with poor human rights records around the world to censor digital speech, including content concerning human rights, health, and religious minorities.[154] A range of other technology and cybersecurity firms like Germany-based FinFisher, Italy-based Hacking Team, and the U.S.-based company Sandvine develop spyware and malware that has likewise been used by governments globally to track human rights activists, journalists, and dissidents.[155] Thus, in explaining its lawsuit, WhatsApp cited the Citizen Lab's work as well as UN Special Rapporteur for Freedom of Expression David Kaye, who called for a moratorium on spyware-enabled "attacks."[156] The post also cited Amnesty International's work and called for "strong legal oversight of cyber weapons like the one used in this attack" to ensure they are not used to violate the rights and freedoms of people "wherever they are in the world."[157]

151. CITIZEN LAB, *supra* note 54.

152. Cathcart, *supra* note 25.

153. *See* Jonathon Penney, Sarah McKune, Lex Gill & Ronald J. Deibert, *Advancing Human Rights in the Dual Use Technology Industry*, 71 COLUM. J. INT'L AFF. 103, 105–07 (2018); *see generally* Anna W. Chan, *The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware*, 44 BROOK. J. INT'L L. 795 (2019).

154. Penney, *supra* note 153, at 103; Chan, *supra* note 153, at 795–97.

155. *See* Penney, *supra* note 153, at 105; Chan, note 153, at 801.

156. WHATSAPP, *supra* note 120.

157. *Id.*

The challenge, of course, is that presently there is almost no legal oversight for spyware, malware, censoring tools, and other forms of "cyber weapons" developed, marketed, sold, and distributed globally by transnational technology companies. Though many of the uses of these tools and technologies directly implicate international human rights law—including provisions in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights[158]—there is no clear avenue where these human rights abuses can be enforced nationally or internationally. International law, for instance, primarily imposes legal obligations on states and state actors, not non-state actors like these companies, thus leaving clear regulatory gaps.[159] And there is no effective international mechanism to hold these companies accountable for human rights abuses.[160] Furthermore, "soft" international law like the UN Guiding Principles on Business and Human Rights, while helpful, remains largely voluntary and provides no new means of accountability.[161] Finally, remedies under domestic law for international victims have also proven largely inadequate.[162] Domestic courts regularly decline jurisdiction, for instance, citing more appropriate venues elsewhere.[163] Though for a time the U.S. Alien Tort Statute provided hope for recourse in American courts, recent Supreme Court decisions have severely limited its scope and application.[164] Finally, the legal basis for states to regulate the extraterritorial activities of businesses is also murky, with international human rights law offering little guidance.[165]

In short, there is a large accountability gap when it comes to technology companies operating internationally and contributing to human rights abuses.[166] The *WhatsApp* lawsuit offers a possible path forward for greater accountability: private sector legal action on behalf of users and victims abroad. Rather than only the targeted victims of abuses having a responsibility to take legal action for remedies and redress, *WhatsApp v. NSO Group* stands as an example of private sector action that advances human

158. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 475–82 (2016); Chan, *supra* note 153, at 802–05.

159. Chan, *supra* note 153, at 805–13; Penney, *supra* note 153, at 104–05.

160. Chan, *supra* note 153, at 806–07; Penney, *supra* note 153, at 104–05.

161. Chan, *supra* note 153, at 809–10.

162. Chan, *supra* note 153, at 811–13; Penney, *supra* note 153, at 104–05.

163. Chan, *supra* note 153, at 811–12.

164. *Id.*; Jonathon Penney, *The Cycles of Global Telecommunication Censorship and Surveillance*, 36 U. PA. J. INT'L L. 693, 742–43 (2015).

165. Penney, *supra* note 153, at 105.

166. Chan, *supra* note 153, at 818–19 (suggesting they have "a bubble of impunity").

rights interests through greater accountability for corporate abuses, not just in the United States, but internationally as well. Though taking us into "uncharted" legal territory,[167] if successful, it may lay the foundation of new possibilities for corporate accountability, beyond mere public shaming via media coverage. This is another good reason to defend the lawsuit.

D. IMPLICATIONS: *VAN BUREN* AND BEYOND

1. Taking the Scope of the Computer System or Service Seriously

There are other implications of our analysis. One is that courts and scholars need to take more seriously the task of theorizing the scope and boundaries of the relevant computer system, service, and the information accessed or obtained. As noted earlier, this has always been an important though neglected issue under the CFAA analysis—you have the define the targeted computer and its scope to determine if someone has accessed it without authorization or exceeded authorizing if already accessing it. After *Van Buren*, the question has arguably become even more important, but also more complex, especially when dealing with attackers with access to the computer system. This is because the Supreme Court's reasoning suggests it favors a code-based approach to access barriers and gates, which means that determining liability depends even more on the contours and nuances of the system or network in question. Now, one needs to understand not just the boundaries of the relevant computer system, but also the different "areas" within it, as a user with authorized access exceeds it only if they bypass an access barrier or gate and reach "other areas" within that system to which their authorized access does not extend.[168]

Yet, this is an issue that courts have often not addressed adequately.[169] In *United States v. Phillips*,[170] for example, the Fifth Circuit found that a University of Texas student accessed a course management website without authorization when he guessed passwords to various faculty and staff accounts on the system.[171] However, the court failed to address the specific computer system that was accessed without authorization.[172] Was it the

167. Newsroom, *supra* note 32.

168. Atlas et al., *supra* note 10; Cunningham, Grant & Hoofnagle, *supra* note 19.

169. Mayer, *supra* note 17, at 1651–53 (noting that "courts have not seriously defined the scope of a computer system…"); Kerr, *supra* note 21, at 1653 (noting the *Morris* case "raised questions about how to divide a network of computers into individual computers for the purpose of the statute," though those issues were ignored by the Second Circuit on appeal).

170. United States v. Phillips, 477 F.3d 215 (5th Cir. 2007).

171. *Id.* at 219–21.

172. *Id.* at 219–21; Mayer, *supra* note 17, at 1652.

course website itself? Each individual account the student accessed? Or the database accessed via the course website? This is important as depending on the answer the magnitude of the hack and the number of "computer systems" accessed without authorization could be substantially different (one website accessed versus multiple user accounts accessed). However, the court did not address the matter.[173] The famous *Morris* case, one of the earliest significant CFAA cases, also involved a similar issue. In that case, Edward Morris, then a Cornell graduate student, was prosecuted for damage caused by his computer worm, which infected computers and spread around the world via the internet.[174] To launch his worm, Morris hacked into a computer at Massachusetts Institute of Technology to conceal its origins.[175] On appeal, a key issue was theorizing and defining the "computer system" at stake. Did Morris engage in a single act of access when he sent his worm over the internet, or was he responsible for every computer that his worm infected thereafter? Also, should the internet, a single network, be divided into individual computers for the purposes of CFAA liability? Unfortunately, again, the Second Circuit did not directly address the issue.[176] After *Van Buren*, both courts and scholars need to take this issue more seriously.

To that end, we have set out a framework for helping determining the scope of the relevant computer system or service and the information therein for CFAA purposes. This "objective" approach takes into account the perceptions of ordinary users; the technical realities of the computer system, service, and information; and the nature of the hack itself. It asks: what was the information the attackers were targeting and what was their methodology? This approach illuminated the proper scope and boundaries of the WhatsApp network, and, looking back, also explains the court's reasoning in the *Mitra* case and how the court treated that network as a whole. We believe it likewise can help arrive at better liability determinations under the CFAA going forward, especially in a post-*Van Buren* world.

2. Theorizing and Defining Access Barrier Circumvention

Another implication is that scholars and courts should take more seriously the task of defining or theorizing what is means to circumvent a code-based access barrier, which has also become increasingly important after *Van Buren*'s narrow construction of the CFAA. Scholars and courts

173. *Phillips*, 477 F.3d at 218; Mayer, *supra* note 17, at 1652.

174. United States v. Morris, 928 F.2d 504, 505–04 (2d Cir. 1991).

175. *See* FBI NEWS STORY, *supra* note 136 (noting Morris hacked into an MIT computer to launch his computer worm).

176. *See* Kerr, *supra* note 21, at 1631, 1631 nn.147–53.

have been prolific in formulating different approaches to "authorized access" under the CFAA, but few have focused systematically on how to theorize different code-based barriers nor parsed what bypassing or circumventing such a barrier requires. Leading scholars like Orin Kerr have argued that the best way to approach code-based access restrictions is as authentication gates, that is, technological measures that require verifying that the user is the person who has access rights to the information accessed,[177] like a portal requiring a password to allow access. This approach has begun to gain traction among courts as well. The U.S. District Court's recent decision in *Sandvig v Barr*[178] held, citing Kerr, that CFAA liability was only triggered only when a defendant bypassed an authentication gate.[179]And there are passages in *Van Buren* suggesting the Supreme Court also favors this approach.[180]

The challenge is that theorizing code-based access barriers only as authentication gates may lead courts to define bypassing or circumvention too narrowly. This is apparent from Kerr's original test for circumvention, which he defined as "tricking the computer" into giving the user "greater privileges" when "computer code" has been used "to create a barrier designed to block the user from exceeding his privileges on the network."[181] This more narrow inquiry neglects how attackers can formulate sophisticated attacks that entirely ignore the authentication function of the code-based barrier and instead wholly circumvent or "workaround" it, rather than tricking the authentication gate into allowing access or exploiting a vulnerability in the gate that gives the attacker greater privileges.[182] One example of such a workaround is to attack the weaker "end points" in the network—like the devices of users—where plaintext versions of unencrypted communications can be obtained.[183] This is especially the case with stronger

177. Kerr, *supra* note 11, at 1146; Kerr, *supra* note 21.

178. Sandvig v. Barr, No. CV 16-1368, 2020 WL 1494065 (D.D.C. filed May 28, 2020), https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/06/Sandvig-v-Barr.pdf.

179. *Id.*

180. Van Buren v. United States, 141 S. Ct. 1648, 1659 n.9 (2021). The Court here cites Bellia. *Id.* But Bellia on the page cited by the court actually cites Kerr for the definition of authorization as authentication. *See* Bellia, *supra* note 69, at 1470 nn.158–59.

181. Kerr, *supra* note 11, at 1146 (both discussing and quoting Kerr, *supra* note 21, at 1644–46). In fairness to Professor Kerr, he later changed this definition to focus on authentication. *See* Kerr, *supra* note 11, at 1146. But even that definition may not work as, here, access arguably did not fall "outside authentication" since the user devices provided authentication; it just happened they were controlled by the attackers. A better way to understand the attack methodology, in our view, is that it aimed to obtain user data and communications by avoiding circumventing the end-to-end encryption on the network itself.

182. Kerr & Schneier, *supra* note 1; Clarke & Ali, *supra* note 3; Squire, *supra* note 8.

183. Kerr & Schneier, *supra* note 1, at 1007–10.

forms of code-based access barriers—like encryption—that are very hard to trick, compromise, or break.[184] Rather, attackers typically seek to work around the encryption, and that is what the attackers did in *WhatsApp v. NSO Group*. But this particular attack likely would not fall into Kerr's definition. Under his test, it would seem the attackers have not circumvented anything—no trickery to fool authentication, credential misappropriation, or hack to pass through the code-based barrier. They have simply carried out a sophisticated "encryption workaround."[185] But this, too, should trigger CFAA liability.

In fairness, Kerr has offered a newer test focused on authentication that is stronger but may also have problems with "work around" attacks. Kerr says the "key point is not that some code was circumvented" but that "the computer owner conditioned access on authentication of the user and the access was outside the authentication."[186] This test was likewise adopted by the court in *Sandvig*.[187] But was access here "outside authentication"? In one sense, yes, in that attackers did not have the cryptographic key to decipher encrypted WhatsApp messages and still gained access. But in a technical sense no, in that messages and other information obtained on the user devices were in plain text; the user had the right credentials for authentication, just the attackers used malicious code to take control of the user's device to avoid dealing with encryption restrictions at all.

One way to avoid these problems is, as we have done in our analysis, to consider the *intended function* of code-based barrier or authentication gate in determining if an attacker has "circumvented" the barrier access or whether access is "outside authentication," to use Kerr's terms, to trigger liability. The "intended function test" was first set out in the famous *Morris* worm case,[188] wherein Edward Morris exploited vulnerabilities in multiple programs, like the SENDMAIL emailing program, that gave him unintended access to areas and information on the system.[189] The court held that he did not use these programs "in any way related to their intended function."[190] We are

184. Kerr & Schneier, *supra* note 1, at 1006–07; Clarke & Ali, *supra* note 3; Squire, *supra* note 8.

185. Kerr & Schneier, *supra* note 1.

186. Kerr, *supra* note 11, at 1164.

187. Sandvig v. Barr, No. CV 16-1368, 2020 WL 1494065 (D.D.C. filed May 28, 2020), https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/06/Sandvig-v-Barr.pdf.

188. United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991); Kerr, *supra* note **Error! ookmark not defined.**, at 1631–32.

189. *Morris*, 928 F.2d at 510; Kerr, *supra* note 21, at 1631–32.

190. *Morris*, 928 F.2d at 510; Kerr, *supra* note 21, at 1631–32.

transplanting this test to a slightly different part of the CFAA analysis—not to understand when access is not authorized, but to understand the nature of code-based barriers and their functions to better understand methods to circumvent them. Indeed, code-based limitations are attempts to enforce an owner's intent to limit authorization through the use of software, hardware, or other technical related measures.[191] Such barriers define not only the limits of access but also communicate the owner's intent to limit access.[192] Thus, we would slightly modify Kerr's test for authentication or circumvention, where liability is triggered when "access is outside authentication or *inconsistent with the intended function of the authentication*." Applying this here shows that the attackers accessed information on user devices *inconsistent* with *its intended function* of end-to-end encryption in the WhatsApp network, which was to protect the privacy and security of WhatsApp user communications from all third parties, including other users in the network. The access was inconsistent with that intended function.

VI. CONCLUSION

In our view, the critical reception to the *WhatsApp* lawsuit—and the CFAA violations it claims—is not justified. If based on our network trespass theory, we believe there is a sound basis for CFAA claims. The *WhatsApp v. NSO Group* casehas the potential to improve corporate accountability for human rights. Our analysis can also lead to better privacy and security outcomes and provides guidance on critical post-*Van Buren* issues. First, our analysis theorizes sophisticated code-based access barriers and their circumvention under the CFAA, including how the law is best applied to encrypted messaging networks and similar social media platforms. Second, it theorizes the scope, boundaries, and areas of the relevant computer system, services, and information therein to determine CFAA liability. These issues have long been neglected by both courts and scholars, but after *Van Buren* that neglect cannot be sustained.

191. Goldfoot & Bamzai, *supra* note 11, at 1487.
192. *Id.* at 1490.