INTERNET TECHNOLOGY COMPANIES AS EVIDENCE INTERMEDIARIES

*Yan Fang**

Search warrants, subpoenas, and other forms of compulsory legal process are essential for legal parties to gather evidence. Internet technology companies increasingly control wide-ranging forms of evidence, yet little is known about how these companies fulfill their compulsory legal obligations. This Article presents an original study of internet technology companies as evidence intermediaries: third-party organizations that control access to evidence routinely sought by legal parties. Drawing on in-depth qualitative interviews with companies' legal and compliance staff and with law enforcement agents, I show how company processes for responding to search warrants cannot be neatly categorized within the existing literature's dichotomy of cooperation or resistance. Rather, the responses consist of makeshift measures that companies have developed to manage predicaments arising from the imprecise or impracticable wording of warrants. These measures can affect the evidence that is ultimately available for use in legal proceedings. They can also untether the scope of searches—as they are carried out—from the procedures of the Fourth Amendment. This Article contends that, because judicial officers are likely ill-

* Assistant Professor of Law, Boston College Law School. For generous feedback and helpful suggestions, I thank Catherine Albiston, Emilie Aguirre, Anne Boustead, Sarah Brayne, Guy Charles, Jim Dempsey, Veena Dubal, Lauren Edelman, Jessica Eaglin, Catherine Fisk, James Graves, Christopher Hoofnagle, Irene Joe, Kate Klonick, Linda Hamilton Krieger, Lawrence Liu, Calvin Morrill, Deirdre Mulligan, Orin Kerr, Christina Koningisor, Osagie Obasogie, Paul Ohm, Yael Plitmann, Diana Reddy, Daniel Richman, Andrea Roth, Alan Rozenshtein, Paul Schwartz, Rachel Stern, Matthew Tokson, Salomé Viljoen, Rory Van Loo, Ari Waldman, Rebecca Wexler, Pauline White Meeusen, and Dvir Yogev. This Article also benefited from discussions at the Culp Emerging Scholars Workshop, the Law and Political Economy Emerging Scholars Workshop, the Privacy Law Scholars Conference, the Law and Technology Workshop, the Junior Technology Law Scholars Workshop, the New Directions in Law and Society Graduate Workshop, the Jurisprudence and Social Policy Forum, the Berkeley Empirical Legal Studies Workshop, and the Law and Society Association Annual Meeting. I also thank the *Virginia Law Review* for superb editorial assistance and the Center for the Study of Law and Society at UC Berkeley, the Center for Long-Term Cybersecurity at UC Berkeley, and the Law and Science Dissertation Grant program (National Science Foundation SBE #2016661) for research funding. Finally, I am grateful to the interview respondents who generously shared their time and experiences with me.

equipped to oversee problematic company practices, a variety of institutional interventions to supplement existing court oversight of search procedure should be considered.

INTRODUCTION

Legal actors depend on forms of compulsory legal process to gather evidence, including information from internet technology companies such as Google, Meta, X (formerly Twitter), and Apple. In 2022, Google and Meta alone received over 230,000 search warrants, subpoenas, and other U.S. compulsory demands.[1] These are nearly all third-party process demands, meaning that the recipient companies are not parties to the underlying disputes. Rather, the companies receive many such demands because their business operations generate evidence relevant to nearly every form of conduct that might give rise to an investigation or legal dispute. For example, congressional committees have subpoenaed companies to obtain social media data related to Russian interference in the 2016 elections.[2] Regulatory agencies submit subpoenas and civil investigative demands to internet technology companies for information about subscribers who have engaged in fraud or been victims of deceit.[3] Litigants in both civil and criminal cases have sought photographs, social media postings, and other forms of data to gather information about witnesses.[4] And perhaps most frequently, law enforcement agents seek evidence from internet technology companies regarding suspects' and victims' identities, communications, and conduct.[5]

[1] See Government Requests for User Data, Meta, https://transparency.fb.com/data/government-data-requests/ [https://perma.cc/SWT6-NA5R] (last visited Apr. 10, 2024) (data showing 125,877 legal process requests received by Meta in the United States in 2022); Global Requests for User Information, Google, https://transparencyreport.google.com/user-data/overview [https://perma.cc/QAA7-PLVH] (last visited Apr. 10, 2024) (data showing 107,306 legal process requests received by Google in the United States in 2022).

[2] Aaron R. Cooper, Congressional Surveillance, 70 Am. U. L. Rev 1799, 1801 (2021).

[3] E.g., Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 140–41 (2007); Rory Van Loo, The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance, 72 Vand. L. Rev. 1563, 1590, 1627 (2019); Andrew Keane Woods, Against Data Exceptionalism, 68 Stan. L. Rev. 729, 776–77 (2016).

[4] See, e.g., Rebecca Wexler, Privacy as Privilege: The Stored Communications Act and Internet Evidence, 134 Harv. L. Rev. 2721, 2738–39 (2021); Joshua A.T. Fairfield & Erik Luna, Digital Innocence, 99 Cornell L. Rev. 981, 1076 (2013); Jane Bambauer, Other People's Papers, 94 Tex. L. Rev. 205, 239 (2015); Marc J. Zwillinger & Christian S. Genetski, Criminal Discovery of Internet Communications under the Stored Communications Act: It's Not a Level Playing Field, 97 J. Crim. L. & Criminology 569, 571 (2007); Steven S. Gensler, Special Rules for Social Media Discovery?, 65 Ark. L. Rev. 7, 9 n.7, 12–13 n.18 (2012).

[5] See, e.g., Slobogin, supra note 3, at 141; Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stan. L. Rev. 99, 147–48 (2018); Anne E. Boustead, Police, Process, and Privacy: Three Essays on the Third Party Doctrine 40 (Aug. 2016) (Ph.D. dissertation, Pardee RAND Graduate School) (on file with RAND Corp.); Am. Bar Ass'n, ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records 2–3 (3d ed. 2013).

Despite the volume and importance of third-party legal process directed at internet technology companies, little is known about how these companies actually undertake the work of processing such demands. To be sure, scholars are aware of the importance of these actors as "evidence intermediaries," which I define as third-party organizations that control access to evidence routinely sought by legal parties. Scholars have paid particular attention to these companies' role in generating and controlling access to information about people, places, and events.[6] For example, a growing body of literature examines the information-centralizing effect of the largest companies—which have vast numbers of users and extensive data from and about those users[7]—as well as those companies' capacity to constrain evidence access.[8] However, with few exceptions,[9]

[6] Jennifer Daskal, The Un-Territoriality of Data, 125 Yale L.J. 326, 328 (2015) [hereinafter Daskal, Un-Territoriality]; Woods, supra note 3, at 731; Paul M. Schwartz, Legal Access to the Global Cloud, 118 Colum. L. Rev. 1681, 1700 (2018); Ian Samuel, The New Writs of Assistance, 86 Fordham L. Rev. 2873, 2884 (2018); Aziz Z. Huq & Rebecca Wexler, Digital Privacy for Reproductive Choice in the Post-*Roe* Era, 98 N.Y.U. L. Rev. 555, 560 (2023); Anne E. Boustead, Hoover Inst., Aegis Series Paper No. 1802, Small Towns, Big Companies: How Surveillance Intermediaries Affect Small and Midsize Law Enforcement Agencies 24 (2018). For implications for defendants, overseas governments, and international bodies seeking evidence, see Wexler, supra note 4, at 2738–39; Alexa Koenig, Keith Hiatt & Khaled Alrabe, Access Denied: The International Criminal Court, Transnational Discovery, and the American Servicemembers Protection Act, 36 Berkeley J. Int'l L. 1, 25 (2018); Kate Westmoreland & Gail Kent, International Law Enforcement Access to User Data: A Survival Guide and Call for Action, 13 Canadian J.L. & Tech. 225, 227 (2015).

[7] E.g., Jon D. Michaels, All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 Calif. L. Rev. 901, 908 (2008) [hereinafter Michaels, All the President's Spies]; Jon D. Michaels, Deputizing Homeland Security, 88 Tex. L. Rev. 1435, 1435–36 (2010) [hereinafter Michaels, Deputizing Homeland Security]; Niva Elkin-Koren & Eldar Haber, Governance by Proxy: Cyber Challenges to Civil Liberties, 82 Brook. L. Rev. 105, 112–13 (2016).

[8] E.g., Rozenshtein, supra note 5, at 105; Kristen E. Eichensehr, Digital Switzerlands, 167 U. Pa. L. Rev. 665, 712–13 (2019); see also Avidan Y. Cover, Corporate Avatars and the Erosion of the Populist Fourth Amendment, 100 Iowa L. Rev. 1441, 1445 (2014) (arguing that service providers cannot serve a government-checking function because they have vested interests in cooperating with the government); Developments in the Law—More Data, More Problems, 131 Harv. L. Rev. 1715, 1722–23 (2018) [hereinafter Developments—More Data] (explaining how technology companies exercise large amounts of discretion in handling law enforcement requests for information, including by minimizing capacity to respond and slowing down response times).

[9] See Orin S. Kerr, The Fourth Amendment Limits of Internet Content Preservation, 65 St. Louis U. L.J. 753, 755 (2021); Christopher Soghoian, The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance 2 (July 15, 2012) (Ph.D. dissertation, Indiana University) (ProQuest); William A. Carter & Jennifer C. Daskal, Ctr. for Strategic & Int'l Stud., Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge 18–19 (2018); Sean E. Goodison, Robert C. Davis & Brian A. Jackson, RAND Corp., Digital

scholars have paid little attention to the core work of the evidence mediating that internet technology companies now undertake: how company staff review demands for evidence, determine what material is responsive, and segregate and produce that material to the demanding party.

This omission is problematic. Current academic accounts focus on companies' highly visible efforts to resist or cooperate with government officials' compulsory demands, such as through litigation against court orders or efforts to encrypt communication services.[10] Moreover, consistent with a focus on companies' publicized activities, existing accounts assume that companies' everyday practices in responding to routine law enforcement evidence demands also reflect a deliberately chosen orientation toward either cooperation or resistance.[11] The focus of existing literature on companies' efforts to obstruct or assist law enforcement overlooks an antecedent problem that companies must navigate: understanding what law enforcement is actually asking of the company.

Internet technology companies represent only half of third-party compulsory legal process. On the other side of this process, law enforcement officers must compose a formal set of directives that would putatively require a company to produce evidence. How agents compose these evidence demands affects how company staff identify and produce that evidence. How those companies actually respond to such directives, in turn, shapes how evidence seekers compose future demands. The highly interrelated character of compulsory legal process suggests that an understanding of companies' roles as evidence intermediaries must account for the two-sided nature of the legal process task, both as a matter of practice and as a matter of theory.

Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence 10 (2015); Michael Vermeer, Dulani Woods & Brian Jackson, RAND Corp., Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers 2 (2018).

[10] Rozenshtein, supra note 5, at 104–05, 115–22; Eichensehr, supra note 8, at 667–68, 677–79; Cover, supra note 8, at 1469–74, 1479, 1481–84; Developments—More Data, supra note 8, at 1722–23; Michaels, All the President's Spies, supra note 7, at 908; Michaels, Deputizing Homeland Security, supra note 7, at 1435–36; Elkin-Koren & Haber, supra note 7, at 112–13.

[11] E.g., Rozenshtein, supra note 5, at 105 (describing a contentious relationship between internet technology companies and law enforcement as the "new normal"). For a critique, see Developments—More Data, supra note 8, at 1724–29.

This Article addresses both these empirical and theoretical requirements. It presents findings from an in-depth interview study that affords substantial insight into internet technology companies' roles as evidence intermediaries for data sought through search warrants. The study involved forty-seven semi-structured interviews with two groups of hard-to-access subjects: company legal and compliance staff responsible for reviewing search warrants and law enforcement investigators and prosecutors responsible for preparing them.

Based on an analysis of these data, I show that in the routine, everyday processing of search warrants, company staff are oriented chiefly toward expedience in processing warrants and only secondarily toward assisting or resisting government efforts to acquire evidence. Indeed, my data indicate that investigators and prosecutors often do *not* prepare search warrants in ways that present the responding company with a choice among actions readily distinguishable as efforts to either facilitate or frustrate agents' access to evidence.

Theoretically, this Article develops the concept of "knowledge misalignment" to explain these findings. Knowledge misalignment arises when the distribution of necessary knowledge among individuals and organizations undertaking a joint task is misaligned with regard to the parts of the task for which each party is responsible. In the context of search warrants for internet evidence, law enforcement agents are well acquainted with the facts of an underlying case, but they often lack the knowledge of the company's operations necessary to compose warrant language that precisely identifies the desired data. This disconnect arises because internet technology companies can easily modify their product and service offerings and thus can collect and store a wide variety of changing data types. As a result, law enforcement agents preparing search warrants often describe desired evidence in terms that reflect incorrect, informal, or outdated understandings of the company's data holdings. The task of interpreting and narrowing imprecise and impractically broad directives then falls to the company staff executing the demand, who may know well what kinds of data their company has but know little about the needs of the underlying investigation beyond what can be inferred from the language of the search warrant.

To manage the task of interpreting and narrowing imprecise and impractically broad warrant directives, company staff use a set of interpretive and technological coping practices. These practices sometimes result in staff producing additional evidence not called for by

the warrant, or failing to produce evidence called for by the warrant. Because these coping practices can displace the terms of search warrants as the measure by which company staff determine the scope of the searches carried out, these practices influence what kinds of evidence, and how much of it, is ultimately available for use in legal proceedings.

Drawing on these insights, this Article also identifies two important implications for legal institutions. First, it identifies a worrisome potential consequence of the practices that companies use to manage knowledge misalignment: these practices can untether the scope of searches, as they are carried out, from the procedures of the Fourth Amendment. Analysis of interview data reveals that when company staff interpret what data are sought in a warrant with a view toward making the production of responsive data a manageable task, they tend to reframe the boundaries of the production in ways that foreground quantitative organizational criteria within their knowledge (e.g., dates, numbers of accounts, data size), rather than the circumstances of the investigation as reflected in the judicially approved language of the warrant. Over time, the production of evidence in response to search warrants may be shaped more by evidence intermediaries' application of these quantitative organizational criteria than an analysis of probable cause that is consistent with the Fourth Amendment.

Second, this Article raises substantial questions about the capacity of our current adversarial system—dependent on judicial oversight of search warrants—to address the knowledge misalignment that underlies potentially problematic company practices. Given that judicial officers are no better informed about the operations of internet technology companies than law enforcement agents, it is difficult to see how resource-constrained judicial officers could acquire an understanding of the data holdings, technical architecture, and production practices of widely ranging businesses that would be necessary to effectively oversee the search warrant response process. All of this points to the necessity of institutional intervention to supplement judicial oversight in individual cases.

This Article proceeds in four Parts. Part I defines the concept of evidence intermediaries and shows how internet technology companies are similar to and different from older evidence intermediaries such as banks, hospitals, and telecommunications companies. Internet technology companies are similar in that they, like other evidence intermediaries, provide centralized access points to evidence. However, these companies

are also distinguishable because they collect broader swaths of data types that change more frequently, they are more opaque to outsiders seeking evidence, and they receive evidentiary demands across a greater variety of cases.

In Part II, I present the design of the interview study that I conducted to examine how internet technology companies process third-party search warrants from law enforcement agencies. Section II.A explains why in-depth interviews with two sets of actors—legal and compliance staff for internet technology companies and law enforcement investigators and prosecutors—are necessary to understand how third-party search procedure for internet evidence works in practice. Sections II.B and II.C summarize the procedures that I used to sample, recruit, and interview respondents and to increase the reliability of the interview data, given that both sets of respondents were reluctant to speak about a sensitive topic that has been the subject of substantial public scrutiny. Section II.D reports what both company and law enforcement respondents emphasized during the interviews: while companies often provide useable evidence in response to search warrants, they encounter uncertainties in understanding what a search warrant is seeking. In response to these uncertainties, companies may end up producing evidence not called for by a warrant *and* withholding evidence that is called for by a warrant.

In Part III, I develop the concept of knowledge misalignment as a diagnosis of a core informational problem in third-party compulsory legal process. Drawing on organizational theory and interview data, I argue that two types of knowledge misalignment complicate company responses to search warrants. *Linguistic misalignment* occurs when search warrants describe the sought-after data in terms that do not align with the data that the company holds or the internal company language used to describe those data. *Substantive misalignment* occurs when company staff must reframe search warrant directives into tasks tractable within the constraints of the company's dedicated resources, without knowledge of the circumstances of the investigation or the legal elements that must ultimately be proven in court. I then explain the four types of practices that companies may use to manage knowledge misalignment: *acquisition* of information about underlying investigations, *reconstruction* of the language of compulsory demands, *standardization* of company staff interpretations of recurring search warrant language, and *insulation* of company knowledge. While these practices allow companies to manage

knowledge misalignment, they also change the nature and quantity of evidence ultimately available to legal parties.

In Part IV, I turn to the institutional implications of these insights. I first explain how the company practices described in my data tend to untether the scope of searches—as they are carried out—from the procedures of the Fourth Amendment. Due to knowledge misalignment, companies usually do not know the facts about the underlying case that gave rise to a given process demand. Thus, when company staff interpret what data are sought in a warrant with a view toward making the production of responsive data a manageable task, they tend to reframe the boundaries of the production in ways that favor handing over routinely produced types of data, often within quantitative limits set by internal company standards. The scope of the search carried out is thus determined not by case-specific assessment of probable cause as determined by a judge and conveyed in the language of the search warrant but rather by makeshift efforts on the part of company staff to apply quantitative organizational limits to search production.

I then argue that judicial officers are likely ill-equipped to oversee the kinds of company practices revealed by the interview data. Similarly to law enforcement agents, judicial officers currently lack the knowledge of internet company data holdings and data production practices that would be necessary to detect and redress the displacement of search warrant directives with companies' standardized internal protocols. Accordingly, I argue for consideration of multiple institutional interventions to supplement judicial oversight.

I. EVIDENCE INTERMEDIARIES

Information technology companies play a variety of intermediary roles.[12] Over the past decade, we have learned about their tremendous power to moderate speech, which has substantial societal consequences for how people see themselves, how they learn about their world, and how they interact with others.[13] The companies also play immense roles in

[12] E.g., Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 137 (2019) (discussing how a "platform-based, massively intermediated information economy is a condition in which fiat-based prohibitions on information flow are both increasingly routine and increasingly inscrutable"); Ashley Deeks, Secrecy Surrogates, 106 Va. L. Rev. 1395, 1401 (2020).

[13] E.g., Evelyn Douek, Content Moderation as Systems Thinking, 136 Harv. L. Rev. 526, 556–57 (2022); Kate Klonick, The New Governors: The People, Rules, and Processes

controlling markets, the livelihoods of individuals, and the fates of small and large businesses alike.[14]

This Part focuses on a different intermediary role now occupied by internet technology companies: their role as evidence intermediaries. Evidence intermediaries are organizations such as hospitals, telephone companies, and banks that perform services that often generate records relevant to a wide range of legal proceedings. These organizations occupy the role of intermediaries because they, rather than the primary legal parties in a proceeding, are routinely responsible for locating, segregating, and producing evidence sought through compulsory legal process. In the search warrant context, for example, after an officer has served a third-party company with a warrant listing various categories of data sought, it is company staff who decide which databases to search, how to search them, and which results to produce.

In this Part, I argue that internet technology companies are a species of evidence intermediary and that several features distinguish them from traditional evidence intermediaries. Section I.A distinguishes third-party evidence intermediaries from first-party evidence producers, who are parties to litigation or direct subjects of investigations and thus have quite different incentives and informational positions in an investigation or case. Section I.B focuses on how the dynamics of compulsory legal process have changed because the particulars of internet technology companies' business activities are broader and more variable, rendering external knowledge of companies' data and evidence more scarce. Section I.C explains how internet technology companies' practices are more opaque to outsiders than those of evidence intermediaries in older industries with more settled and regulated businesses.

In Section I.D, I argue that, to understand internet technology companies' role as evidence intermediaries, we must focus on the companies' interactions with evidence seekers. This emphasis is necessary because the work of mediating evidence is interrelational and

Governing Online Speech, 131 Harv. L. Rev. 1598, 1600–01 (2018); cf. Sarah T. Roberts, Behind the Screen: Content Moderation in the Shadows of Social Media 33–34 (2019) (discussing the role that companies play in content moderation on their websites and platforms).

[14] Rory Van Loo, The Corporation as Courthouse, 33 Yale J. on Regul. 547, 551, 566, 583–84 (2016); Rory Van Loo, Federal Rules of Platform Procedure, 88 U. Chi. L. Rev. 829, 830–31 (2021); K. Sabeel Rahman & Kathleen Thelen, The Rise of the Platform Business Model and the Transformation of Twenty-First-Century Capitalism, 47 Pol. & Soc'y 177, 187 (2019).

depends substantially on the types of data that the organization holds and the legal parties seeking those data.

A. Defining Evidence Intermediaries

Evidence intermediaries are third-party organizations that control access to evidence routinely sought by legal parties. Unlike individuals, who are also frequent sources of evidence, evidence intermediaries are organizations whose records and databases contain information about many people or events that are often relevant to legal parties conducting investigations or undertaking litigation. As such, these types of organizations, through their decisions and actions, likely have a more significant impact across a greater range of cases than any individual.

Evidence intermediaries also tend to have more of a prerogative with respect to the evidence sought. Unlike parties to litigation, evidence intermediaries are not already under the supervision of a court presiding over a lawsuit. While litigants and investigation targets face the risk that withholding evidence will expose them to negative consequences, including adverse inferences,[15] third-party evidence intermediaries typically do not face these risks. This is because evidence intermediaries' core connection to the events being litigated or investigated is their possession of potentially relevant records.

Further, while litigants and investigative targets may have strong reasons *not* to produce evidence relevant to another party,[16] evidence intermediaries' interests are less clear-cut. On the one hand, as they are nonparties, there is no overall reason to suspect that evidence intermediaries want to intentionally frustrate particular investigations or litigation in the way that parties to a dispute may. On the other hand, searching, segregating, and producing data costs time and money. As third parties, evidence intermediaries may seek to produce less information—or produce information less selectively—to reduce the resources involved in meeting their obligations to comply with compulsory legal process.

To be sure, evidence intermediaries do face some risk of litigation or reputational harm arising from their evidence production decisions.

[15] E.g., Dale A. Nance, Adverse Interferences About Adverse Inferences: Restructuring Judicial Roles for Responding to Evidence Tampering by Parties to Litigation, 90 B.U. L. Rev. 1089, 1090 (2010); Charles W. Adams, Spoliation of Electronic Evidence: Sanctions Versus Advocacy, 18 Mich. Telecomm. & Tech. L. Rev. 1, 53 (2011).

[16] E.g., Edith Beerdsen, Discovery Culture, 57 Ga. L. Rev. 981, 1050 (2023); Frank H. Easterbrook, Discovery as Abuse, 69 B.U. L. Rev. 635, 638–39 (1989).

Moreover, they may have genuine concerns about keeping customers' and users' information away from litigants, particularly government agencies, whose evidence gathering invokes the specter of government surveillance. Indeed, historically, telephone companies, banks, and hospitals have challenged various forms of third-party legal process.[17] However, as parties that are neither litigants nor investigative targets, their focus is much more likely to center on the work involved in producing responsive data rather than the substantive valence of the data ultimately produced.

B. Distinguishing Internet Technology Companies

Evidence intermediaries are not a new phenomenon. Hospitals, for instance, have functioned for decades as centralized points for investigators to access individuals with acute medical or psychiatric needs and their medical records.[18] Banks and credit card companies similarly serve as intermediaries between legal parties and customer financial information of a kind routinely sought for use in civil, criminal, and regulatory proceedings.[19] Telecommunications companies have long mediated between government officials and the companies' networks, which afford a centralized, third-party access point for evidence about

[17] See, e.g., Dongsheng Zang, Telegraph, Telephone and the Internet: The Making of the Symbiotic Model of Surveillance States, 40 Ariz. J. Int'l & Compar. L. 1, 12–13 (2023); Reps. Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1038 (D.C. Cir. 1978); United States v. First Nat'l Bank, 295 F. 142, 143 (S.D. Ala.), *aff'd per curiam*, 267 U.S. 576 (1924) (rejecting third-party bank challenge of IRS summons for testimony and records concerning customers); cf. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 45, 77 (1974) (upholding the passage of the Bank Secrecy Act of 1970 in light of plaintiff California Bank Association challenging its constitutionality under the First, Fourth, and Fifth Amendments); Dan Eggen, Doctors, Hospitals Challenge U.S. Subpoenas, Wash. Post (Feb. 12, 2004, 12:00 AM), https://www.washingtonpost.com/archive/politics/2004/02/12/doctors-hospitals-challenge-us-subpoenas/68bb3127-92b2-4b8b-ae9d-7d9ccb78cea1/ [https://perma.cc/TY9X-C5EH] (detailing a group of physicians and hospitals challenging subpoenas for patient information made by the Justice Department).

[18] Ji Seon Song, Policing the Emergency Room, 134 Harv. L. Rev. 2646, 2647 (2021); Am. Hosp. Ass'n & Nat'l Ass'n of Police Orgs., Guidelines for Releasing Patient Information to Law Enforcement 1, 3, https://www.aha.org/system/files/2018-03/guidelinesreleasinginfo.pdf [https://perma.cc/7Y4P-GWKR] (last visited Apr. 8, 2024).

[19] Cf. Woods, supra note 3, at 776–77 (discussing how balancing interests among sovereign states has led to judicial decisions to compel overseas banks to release customer information); *Cal. Bankers Ass'n*, 416 U.S. at 25–26 (1974) (detailing the legislative history of the Bank Secrecy Act of 1970, which addressed the unavailability of bank records of customers thought to be undertaking illegal activities); United States v. Miller, 425 U.S. 435, 436 (1976) (holding the Fourth Amendment did not apply to defendant's bank records).

people's communications.[20] Like all these organizations, internet technology companies can mediate evidence because when law enforcement agents serve such a company a search warrant, the agents themselves do not search the company's databases.[21] Organizations in this sector provide widely used services that entail collecting and retaining information about what has been done by or to their customers, and those organizations have, in turn, found themselves routinely obliged to produce that information as evidence for a wide variety of investigations and legal proceedings.

Nonetheless, the rise of internet technology companies has substantially changed the realities of compulsory legal process in ways that go beyond amplifying existing dynamics.[22] Several characteristics distinguish internet technology companies from traditional evidence intermediaries like banks and hospitals. First, internet technology companies change products, services, and data holdings more rapidly. Second, because the core business of these companies often consists largely or entirely of the collection and exploitation of data, the variety of data types they collect tends to be both greater and more difficult to anticipate than that of traditional evidence intermediaries, whose data collection is often incidental to carrying out better-understood services. Third, it is more difficult for external actors to learn what types of data an internet technology company has, or how these data are organized within the company's holdings—matters about which internet companies tend to be quite secretive. Fourth, the companies may receive more evidence demands from many more types of legal parties. This set of features makes internet technology companies particularly important evidence intermediaries. Not only do they control evidence important to an

[20] *Reps. Comm.*, 593 F.2d at 1038; Zang, supra note 17, at 18, 20–21; Michaels, Deputizing Homeland Security, supra note 7, at 1447–51; Goodison et al., supra note 9, at 10; Peter Swire, From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, 2 Int'l Data Priv. L. 200, 204 (2012).

[21] See Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1211 (2003) ("Because ISPs are third-party corporate entities, investigators do not ordinarily search the servers of ISPs directly. Investigators do not break down the ISP's door and start looking for the files themselves. Instead, they obtain a court order compelling the network provider to disclose the information to the government.").

[22] See Rozenshtein, supra note 5, at 105 ("By entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of *surveillance intermediaries*: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance.").

expanded range of legal disputes, but they also control much of the information about their own data holdings necessary to identify and demand that evidence through compulsory legal process.

1. Frequently Changing Data Types

Internet technology companies are set apart from traditional evidence intermediaries in that their products and services, as well as the types of data that they collect, change much more frequently. This is because the core business of many such companies is to develop software applications—typically those running on web browsers, mobile devices, and computers—whose features can be revised with varying degrees of ease.[23] As such, internet technology companies can readily modify their products and services, constantly adjusting the features and backend processes of particular applications,[24] as well as rapidly introducing or discontinuing products, services, and features.[25] And even when there are no visible changes to the consumer-facing dimensions of a product or service, companies can readily change the backend functions through which data is collected, stored, and used.[26] As a result, the data that companies collect and keep can be changed much more frequently, as companies improve their own understanding of how to exploit data collected by their products and services.

The varying scope and nature of companies' products and services—combined with changing purposes and practices for collecting, storing, transmitting, and using data—has two important implications. First, there

[23] See Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 153 (2018) (discussing sudden changes to Facebook's news feed feature); Ari Ezra Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power 198–205 (2021) (discussing ways in which companies design and change product features to increase consumers' engagement and disclosure of personal information).

[24] For example, companies can incorporate end-to-end encryption or "disappearing data" features into products and services, making customer data difficult or impossible to access. Orin S. Kerr & Bruce Schneier, Encryption Workarounds, 106 Geo. L.J. 989, 990 (2017); Rozenshtein, supra note 5, at 109; Agnieszka McPeak, Disappearing Data, 2018 Wis. L. Rev. 17, 19; Samuel J. Rascoff, Presidential Intelligence, 129 Harv. L. Rev. 633, 662–65 (2016).

[25] Swire, supra note 20, at 200, 205.

[26] Firms can also reduce government access by storing minimal amounts of customer data, storing data outside of a particular country, or storing data in ways that make it impossible to pinpoint the exact geographic location of those data. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677, 719 (2014); Jennifer Daskal, Borders and Bits, 71 Vand. L. Rev. 179, 180–81 (2018); Jennifer Daskal, Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, 8 J. Nat'l Sec. L. & Pol'y 473, 473 (2016); Daskal, Un-Territoriality, supra note 6, at 328; Schwartz, supra note 6, at 1681.

is simply more knowledge that outside legal actors must acquire about internet technology companies, compared to other evidence intermediaries. Second, even as outside evidence seekers become familiar with a company's data practices—for example, through repeated usage, transactions, and interactions—their knowledge becomes outdated due to the tendency of such companies to quickly change their products, services, and data holdings.[27] Thus, even if evidence seekers gain a good sense of what data companies have or what companies do with it, the accuracy of that knowledge tends to attrit as companies change the features of long-standing products, develop new products, and discontinue older ones.

2. Greater Variety of Data Types

As noted above, the collection and analysis of data by traditional evidence intermediaries is often incidental to their core, better-understood business or service, such as banking, telephony, or medical care. Because internet technology companies may seek to collect and exploit data for their own sakes, independent of the provision of goods and services—these companies tend to gather many more *kinds* of information—often about vastly *greater* numbers of people, often across a much broader range of their everyday activities.[28]

Health organizations, for example, collect information relevant to or arising from the provision of medical or psychiatric care, and the types of data they have and how it is organized typically reflect that focus, for example, by centering on the causes and symptoms of patients' ailments, or the nature, timing, and justification of the healthcare provider's efforts to diagnose, palliate, and treat those ailments. Although now digitized and stored in electronic health records, the data making up their treatment

[27] Cf. Swire, supra note 20, at 205 ("Even when government agencies temporarily learn how to gain access to a particular product or service, the rate of innovation on the Internet remains high—when a new game or a new version of a game is issued, the access that worked previously may no longer succeed.").

[28] E.g., Cohen, supra note 12, at 6; Nancy S. Kim & D.A. Jeremy Telman, Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent, 80 Mo. L. Rev. 723, 726, 728, 735 (2015); Rozenshtein, supra note 5, at 113–15, 117; Michaels, All the President's Spies, supra note 7, at 901, 908; Michaels, Deputizing Homeland Security, supra note 7, at 1435.

records are often still retrievable according to the patient or chronological events in which tests, diagnoses, and treatments were made.[29]

Evidence seekers thus usually have a fairly good sense of the nature of the services that hospitals or medical offices provide and accordingly, of the general types of information that those organizations would possess. By contrast, the variety of products and services offered by internet technology companies—and the aspects of their users' lives through which those products generate data—tend to be novel relative to traditional evidence intermediaries and also vary significantly across companies, such that it is more difficult for those seeking evidence to understand or predict what types of data an internet technology company will have or how those data may be organized.

As a result, although internet technology companies generate a great deal of data about nearly every person who regularly uses a computer or cellular phone, the nature of those data, exactly which companies have them, and which aspects of the user's everyday life they record vary significantly from one company to the next. Thus, the expanded volume and variety of data that internet technology companies record and retain regarding individuals makes it likely that successfully investigating something done by or to a person will entail seeking evidence from an internet company. Because companies' services vary—and consumers may in turn use their services in differing ways—it is likely that an evidence seeker may lack experience using the products of the company from which the investigator needs information.

3. Organizational Opacity

Internet technology companies are also more opaque than traditional evidence intermediaries. First, as organizations whose core business is entirely, or at least largely, dependent on the development of software to collect, store, and exploit data, internet technology companies tend to be secretive about their data practices. During litigation, even as third parties, internet technology companies routinely use trade secrets, contractual terms, and nondisclosure orders to prevent information about their

[29] See, e.g., Craig Konnoth, Health Data Federalism, 101 B.U. L. Rev. 2169, 2184–85 (2021). Bank records, also long since digitized, also tend to be collected and ordered according to account-holder identity and legally mandated data types associated with storing and transmitting financial funds. See Raúl Carrillo, Seeing Through Money: Democracy, Data Governance, and the Digital Dollar, 57 Ga. L. Rev. 1207, 1238–42 (2023).

business and data practices from being made public.[30] More generally, companies may fear that disclosures would give competitors an advantage or give regulators, investors, and consumers more information about company practices.[31] As Sonia Katyal aptly puts it, "private businesses now play the roles that government used to play, but are able to utilize the principles of trade secret law to protect themselves from the very expectations of transparency that the government operated under."[32]

Traditional evidence intermediaries are also more visible to outsiders because they are more regulated than internet technology companies. This greater regulation pushes traditional intermediaries such as hospitals and banks to have more systematic business practices and to produce more public information about their operations. For instance, banks, hospitals, and telecommunications companies require licenses to operate and are subject to periodic inspection and monitoring by regulators, including inquiries into their data and record management practices.[33] Many of these organizations are also subject to various information retention and

[30] Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343, 1343 (2018); cf. Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 136–38 (2017) (describing how overseeing big data is a difficult endeavor given the specialized knowledge required to understand proprietary predictive algorithms); Elizabeth E. Joh, The Undue Influence of Surveillance Technology Companies on Policing, 91 N.Y.U. L. Rev. Online 101, 101 (2017) (demonstrating "the increasing degree to which surveillance technology vendors can guide, shape, and limit policing in ways that are not widely recognized").

[31] See Wendy Wagner & Will Walker, Incomprehensible!: A Study of How Our Legal System Encourages Incomprehensibility, Why It Matters, and What We Can Do About It 20–21 (2019) (discussing how companies may be incentivized against meaningful communication in order to confuse or mislead consumers and regulators); Frank H. Easterbrook & Daniel R. Fischel, Mandatory Disclosure and the Protection of Investors, 70 Va. L. Rev. 669, 685–86 (1984) (discussing how firms may not want to disclose information that would benefit rival firms and their investors); Jeffrey Pfeffer & Gerald R. Salancik, The External Control of Organizations: A Resource Dependence Perspective 105 (1978) (noting how the disclosure of information is a "major source[] of conflict between organizations which wish to influence and the organizations which seek to avoid influence and maintain discretion").

[32] Sonia K. Katyal, Private Accountability in the Age of Artificial Intelligence, 66 UCLA L. Rev. 54, 118–19 (2019).

[33] E.g., Van Loo, supra note 3, at 1620; Whitfield Diffie & Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption 174 (2d ed. 2007); Zang, supra note 17, at 26–27; Reps. Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1036 (D.C. Cir. 1978) (discussing data kept by telephone companies for billing purposes); cf. Denise L. Anthony, Ajit Appari & M. Eric Johnson, Institutionalizing HIPAA Compliance: Organizations and Competing Logics in U.S. Health Care, 55 J. Health & Soc. Behav. 108, 108 (2014) (stating that "[h]ealth care is one of the most regulated industries in the United States").

reporting requirements.[34] For example, medical professionals must report gunshot wounds, sexual assaults, intimate partner violence, and child abuse,[35] while banks must report suspicious activity reports and comply with know-your-customer laws.[36] In contrast, most internet technology companies are not subject to information retention or reporting obligations outside of two circumstances: when they become aware of sexual crimes against children[37] and when they receive preservation letters relating to specific users or accounts under investigation.[38] This relatively permissive regulatory environment for internet technology companies provides them greater flexibility to modify products, services, and data-collection and data-keeping practices, such that even investigators with repeated prior experience using data from the companies may be poorly informed regarding a company's current data practices. The lack of general data retention and reporting obligations also reduces pressure to instill more uniformity and transparency in companies' data holdings and management practices.

Some of the opacity also results from internet technology companies' relative youth. For both evidence seekers and evidence-producing companies, there is a shorter institutional memory of interactions together. For instance, the passage and implementation of the Communications Assistance for Law Enforcement Act of 1994 involved

[34] See H. Jeff Smith, Managing Privacy: Information Technology and Corporate America 22–24 (1994) (describing the emergence of privacy regulations for U.S. banks, including the Bank Secrecy Act of 1970).

[35] Song, supra note 18, at 2663; Ji Seon Song, Cops in Scrubs, 48 Fla. St. U. L. Rev. 861, 873–76 (2020); Sunita Patel, Transinstitutional Policing, 137 Harv. L. Rev. 808, 868 (2024); Kaaryn Gustafson, The Criminalization of Poverty, 99 J. Crim. L. & Criminology 643, 698 (2009); Khiara M. Bridges, The Poverty of Privacy Rights 4–6 (2017); cf. Elizabeth Chiarello, The War on Drugs Comes to the Pharmacy Counter: Frontline Work in the Shadow of Discrepant Institutional Logics, 40 Law & Soc. Inquiry 86, 86 (2015) (detailing how interviews with retail pharmacists revealed that they operated as dual gatekeepers, making decisions that would be consequential to customers' healthcare and potential criminal liability).

[36] Under various laws, banks must keep detailed personal data on each customer and submit reports about suspicious activities; they are audited and monitored by regulators for their data-keeping and reporting practices. See, e.g., John J. Byrne, The Bank Secrecy Act: Do Reporting Requirements Really Assist the Government?, 44 Ala. L. Rev. 801, 809–12 (1992); Paul B. Rasor, Controlling Government Access to Personal Financial Records, 25 Washburn L.J. 417, 430–35 (1985).

[37] Companies are legally required to report known child sexual exploitation materials to the National Center for Missing and Exploited Children, which then forwards the report to one or more agencies. 18 U.S.C § 2258A.

[38] Id. § 2703(f).

sustained negotiations—and conflicts—between law enforcement agencies and telecommunications carriers regarding the types of data that companies must be able to collect and produce at the behest of agencies.[39] Mandatory reporting obligations for hospitals, pharmacies, and banks also create more opportunities for those organizations to interact with law enforcement and regulatory and private litigants over time.[40] The longer history and greater frequency of interactions mean that law enforcement agencies and other types of organizations have had substantially greater opportunities to cultivate a mutual stock of knowledge about what sorts of data the companies have and what sorts of data evidence seekers typically need.

Finally, some of the opacity results from the difference in internet technology companies' relationships with and awareness of their users relative to those of long-established evidence intermediaries, which traditionally have had more in-person contact with individual users during transactions that entailed collecting and verifying multiple pieces of identifying information (e.g., driver's licenses, account numbers, mailing and residential addresses). Internet technology services often permit users to sign up for accounts relatively quickly—and often for free—with little identifying information. Thus, for many services, one person can set up multiple accounts. These factors also mean that when evidence is sought from internet technology companies, it often is not readily apparent which account or accounts correspond to the suspect user or users identified in the search warrant, prompting concern that the data production that the warrant calls for would entail disclosing information about a user with no connection to the investigation or with a name or username similar to the suspect's rather than about the accounts actually connected to the suspect conduct.

4. Variation in Demands

The variability, scope, and opaqueness of internet technology companies' data—both across time and across companies—also has consequences for companies, as recipients of third-party compulsory legal process. Compliance staff at institutions such as banks and hospitals

[39] Diffie & Landau, supra note 33, at 209, 220; Albert Gidari, Jr., Keynote Address—Companies Caught in the Middle, 41 U.S.F. L. Rev. 535, 542, 544 (2007).

[40] Internet technology companies also tend to lack frontline offices or physical locations that evidence requesters can easily access, which limits the opportunities for face-to-face interactions between evidence seekers and company representatives.

that focus on relatively similar types of products and services often have a better sense of the kinds of investigations that give rise to demands for company records, or at least of the purpose for which those records will be used—for example, to trace the movement of money or establish the condition of a person's body at a particular time. Matters differ for internet technology companies, whose products can touch almost all aspects of users' lives. The data holdings of such companies include evidence that can be relevant in a wide variety of ways to nearly every form of conduct that is subject to investigation, such that compliance staff are less likely to develop a reliable sense of what is generally needed by investigators who seek evidence from them.

C. Evidence Mediation as an Interrelational Process

For all the reasons identified above, internet technology companies are a different type of evidence intermediary from those traditionally encountered by legal parties. And as a distinct type of evidence intermediary, it is important to understand how such companies relate to the various legal actors who seek evidence from them. Critically, the above analysis suggests that the work of evidence intermediaries is not unitary but interrelational: they mediate between legal actors and evidence in the course of repeated transactions. Thus, the work of third-party compulsory legal process requires, to a degree, that evidence seekers have knowledge about the evidence intermediary as an organization and the data it holds and that intermediaries know something about the data being sought. Understanding how internet technology companies actually operate as evidence intermediaries, then, requires a research study that examines the interplay—across individual evidence demands as well as from one demand to the next—between the legal parties seeking evidence from companies and the company staff who respond to these demands.

II. METHODS AND FINDINGS

How do internet technology companies respond to routine third-party evidence demands? I turn to this question in this Part, which presents the design and findings of an in-depth qualitative interview study with current and former company legal and compliance staff who review evidence

demands, and with current and former law enforcement investigators and prosecutors who seek evidence from companies.[41]

The study focused on how companies respond to search warrants because warrants are arguably the most powerful form of compulsory legal process, entitling officers to search for and seize all items authorized in the warrant. Further, under the federal Stored Communications Act ("SCA"),[42] a search warrant can obtain a greater range of stored data types,[43] including basic subscriber information,[44] record and other non-content information,[45] and communications content including substantive messages themselves.[46] In contrast, under the SCA, subpoenas may be used only to access basic subscriber information, while certain court orders can solicit access to additional non-content records and information.[47] Neither subpoenas nor court orders are legally authorized to obtain content information.[48] Because search warrants can access all forms of stored data, they are also an important case to understand how internet technology companies—with a greater variety of frequently changing data types—respond to other forms of third-party compulsory legal process that are less powerful.

As discussed above, third-party search procedure for internet evidence is an interactional process: searches occur as a result of two sets of organizations' actions affecting each other's ability to complete their respective parts of the task. As such, joint consideration of the perspectives of the evidence seekers *and* evidence producers will tend to best illuminate how the process works.

Here, the evidence seekers are law enforcement investigators and prosecutors. Investigators are sworn law enforcement personnel

[41] The research involving human subjects was approved by the UC Berkeley Committee for Protection of Human Subjects.

[42] 18 U.S.C. §§ 2701–2713. Under the SCA, any stored information—whether subscriber information, transactional information, or content information—can be obtained via a search warrant. Kerr, supra note 21, at 1221–23.

[43] 18 U.S.C. § 2703(a)–(c).

[44] Id. § 2703(c)(2) (such as names, addresses, or credit card numbers used to pay for services, or the types of services used).

[45] Id. § 2703(c)(1) (such as network logs of events and transactions that occur on a server).

[46] Steven M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell, It's Too Complicated: How the Internet Upends *Katz*, *Smith*, and Electronic Surveillance Law, 30 Harv. J.L. & Tech. 1, 22–23 (2016); Kerr, supra note 21, at 1218–19.

[47] 18 U.S.C. § 2703(c)(1)–(2).

[48] Some courts have ruled that litigants can obtain content information that is publicly posted or which consumers have consented to release. E.g., Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 728 (Cal. 2018).

responsible for completing follow-up investigations of crimes not solved by patrol officers.[49] Investigators have two primary responsibilities: identifying suspects and collecting and preserving evidence. The latter includes interviewing witnesses, coordinating lab work processing, and requesting documentary evidence,[50] including through search warrants for internet evidence. Investigators also work directly for county district attorneys' offices, where they collect evidence not originally gathered by a responding officer and also initiate investigations. Prosecutors typically enter investigations later in the process. County prosecutors usually do not apply for search warrants directly, but they sometimes play a role in reviewing search warrant applications.[51] In federal investigations, Assistant U.S. Attorneys play an extensive role in reviewing applications from investigating agents and obtaining judicial approval.

At companies, the evidence producers are typically legal and compliance professionals responsible for reviewing compulsory legal process. These individuals work within or adjacent to legal, compliance, and operations departments, often called "law enforcement response," "law enforcement operations," "investigations support," "subpoena compliance," and "trust and safety" teams. The lawyers who lead teams often have titles such as "director" or "counsel," while nonlawyer leaders often have "manager" titles. Nonlawyer reviewers usually do the frontline work of responding to legal process requests, and their titles include "assistant," "associate," "analyst," or "specialist." Reviewers with more experience also have titles such as "lead."[52]

I used in-depth interviews because they are well suited for investigating social processes and understanding the impressions, views, and perspectives of interview participants.[53] For example, company staff who do the routine work of responding to legal process demands can speak to

[49] Anthony Braga, Edward Flynn, George Kelling & Christine Cole, Moving the Work of Criminal Investigators Towards Crime Control, New Persps. Policing, Mar. 2011, at 1, 4, https://www.ojp.gov/pdffiles1/nij/232994.pdf [https://perma.cc/AG3H-5GZK].

[50] Id. For empirical research on criminal investigations, see Peter W. Greenwood & Joan Petersilia, 1 The Criminal Investigation Process: Summary and Policy Implications 7–10 (1975); Frank Horvath, Robert T. Meesig & Yung Hyeock Lee, A National Survey of Police Policies and Practices Regarding the Criminal Investigations Process: Twenty-Five Years After RAND 23 (2001).

[51] See Richard Van Duizend, L. Paul Sutton & Charlotte A. Carter, The Search Warrant Process: Preconceptions, Perceptions, Practices 20–21, 95–97 (1953).

[52] See infra Table 6.

[53] Robert Stuart Weiss, Learning from Strangers: The Art and Method of Qualitative Interview Studies 1–11 (1995).

how they and their teams review warrants and what interactions they have with investigators. Likewise, investigators can speak to the types of data that they receive in response to warrants and their interactions with company staff. Both the similarities and the differences in the accounts reported by the different categories of respondents allow the researcher to identify tensions in interactions and ways in which the parties have worked through those challenges.

Qualitative interviews also provide valuable information about the perspectives of the relatively powerful, who often receive less study than those with less power.[54] Such interviews can be a crucial—and sometimes the only—source of information for studies involving questions of power relationships.[55] In the instant context, which is often marked by secrecy and unwillingness on the part of both companies and law enforcement to discuss their work openly, interviews allow researchers to build rapport with participants during the interview. This rapport is essential to learning about the concrete challenges that people encounter in their work and the ways they approach managing these challenges. The focus on search warrants also alleviated some participants' concerns about speaking with researchers. Search warrants are *the* constitutionally prescribed method for government actors to gather evidence. Thus, discussing their experiences with warrants could feel less risky to participants than discussing their experiences with other types of compulsory orders because there is little question about the legality of companies' producing data in response to warrants.

A. Research and Triangulation Interviews

Because of the sensitivity of this subject area for law enforcement agents and company staff alike, I conducted two different types of interviews: research interviews and triangulation interviews. The forty-seven research interviews that I conducted were the sole means of data

[54] Laura Nader, Up the Anthropologist—Perspectives Gained from Studying Up, *in* Reinventing Anthropology 284, 301–08 (Dell Hymes ed., 1974).

[55] Rebecca S. Natow, The Use of Triangulation in Qualitative Studies Employing Elite Interviews, 20 Qualitative Rsch. 160, 160 (2020) ("An 'elite' is an individual who holds or has held some powerful position that has afforded the individual unique knowledge or information from a privileged perspective."); Adrianna Kezar, Transformational Elite Interviews: Principles and Problems, 9 Qualitative Inquiry 395, 412 (2003); Robert J. Thomas, Interviewing Important People in Big Companies, *in* Studying Elites Using Qualitative Methods 3, 4–6 (Rosanna Hertz & Jonathan B. Imber eds., 1995).

collection.[56] The research interviewees agreed to have their interview responses used in publications and presentations without attribution and with several measures in place to protect their anonymity.[57] Thirty-six of the research interviewees permitted me to record and transcribe their interviews.[58] The mean duration of the research interviews was one hour and forty-three minutes.

I also conducted an additional thirteen triangulation interviews designed to serve as a comparison for the interviews with research respondents.[59] "Triangulation" refers broadly to using multiple sources of evidence or multiple analytic techniques to obtain a more complete understanding of the phenomenon under investigation.[60] Given the sensitive topic under study, the triangulation interviews were necessary to corroborate the research interview data.[61] The triangulation interviews also helped me to ascertain the range of subtopics to cover during the research interviews, identify topics that research interviewees omitted discussing altogether or tended not to raise on their own initiative, and pointed me to informative publicly available materials, such as cases, news articles, and press releases. I did not find systematic differences between the information reported during triangulation and research interviews. None of the triangulation interviews were recorded, and none of the data quoted or paraphrased in this Article are drawn from these interviews.

B. Sampling and Recruitment

To identify individual respondents, I used multiple sampling strategies: random, convenience, niche, and snowball. Random sampling was important to identify companies participating in search procedure but less

[56] See infra Table 1. I conducted twenty research interviews with company staff and twenty-seven research interviews with investigators and prosecutors.

[57] Consistent with my protocol approved by the UC Berkeley Committee for the Protection of Human Subjects, I explained to research respondents that I would not use their name or the names of their present or past employers and that if I paraphrased, quoted, or excerpted their interview responses, I would remove or change the identifying characteristics and the names of participants and organizations.

[58] See infra Table 4.

[59] I conducted eight triangulation interviews with company reviewers and five triangulation interviews with law enforcement. See infra Table 1.

[60] Natow, supra note 55, at 160–61.

[61] Philip H.J. Davies, Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services, 21 Politics 73, 77–79 (2001).

known to the public and scholars.[62] To facilitate the random sampling, I focused on interviewing investigators and prosecutors for law enforcement agencies in California.[63] At the start of the study, California was the only state requiring the annual release of data on a subset of search warrants issued to technology companies, which permitted random sampling of companies and law enforcement agencies.[64]

To identify particular companies, I drew a random sample of fifty-four technology companies identified in a 2016–2020 public data set of search warrants released by the California Department of Justice.[65] I estimated that contacting fifty-four companies would facilitate access to at least five to seven companies of varied sizes and in different sectors. I then used cold outreach,[66] as well as convenience, niche, and snowballing sampling, to identify particular staff persons to contact.[67] A variety of methods were

[62] Existing scholarship and commentary focus on litigation and well-publicized conflicts between companies and law enforcement. See supra text accompanying notes 1–6.

[63] Focusing on agencies from one state also facilitated controlling for significant variations in state law, such as in criminal procedure, evidence, privacy, and criminal law, which may affect how law enforcement agents draft warrants and, thus, how companies respond to those warrants.

[64] Any criminal law enforcement agency in California that executes a warrant or obtains information in an emergency from an electronic communications service provider is required to notify the identified target(s) of the warrant or emergency request. Cal. Penal Code § 1546.2(a)(1) (West 2024). If an agency is unable to identify the target, the agency must notify the California Department of Justice. Id. § 1546.2(c). Under California law, an electronic communications service provider is an entity that provides users the ability to send or receive "electronic communications," defined as the "transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature" by "a wire, radio, electromagnetic, photoelectric, or photo-optical system." Id. § 1546(c), (e), (j). This broad definition covers firms that provide cellular phone, social media, storage, and email services, among others. Susan Freiwald, At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA), 33 Berkeley Tech. L.J. 131, 147–48 (2018).

[65] State of Cal. Dep't of Just., Data Portal: Electronic Search Warrant Notifications, https://openjustice.doj.ca.gov/data [https://perma.cc/TM62-UYKJ] (last visited Apr. 8, 2024).

[66] For cold outreach, I used LinkedIn Premium to search for people who worked at those companies and whose LinkedIn profiles included the word "warrant," "subpoena," "court," "legal process," "ECPA," "law enforcement," "operations," "compliance," "security," or "safety." I reviewed each profile result and identified people whose titles or profiles seemed most relevant. I sent LinkedIn messages to one to three individuals for each company, including individuals in frontline and manager roles where found. For companies whose searches resulted in dozens of profiles, I contacted every fifth profile.

[67] In addition to random sampling, I reached out to people in my professional network who worked at the sampled companies (convenience sampling); attended legal conferences, talks, and panels where I met potential respondents or contacts (niche sampling); and asked both research and triangulation respondents if they would contact colleagues who might be willing to participate in the study (snowball sampling). Each of these three methods also involved

needed to increase the chances of generating richer and more reliable data through interviews, which are, ultimately, social interactions involving the researcher and respondent. Some respondents may be more willing to speak frankly if the researcher is introduced via a trusted, mutual contact.[68] Other respondents, in contrast, are more comfortable speaking to a stranger. Identifying respondents via a variety of methods increased the chances of successful recruitment and forthcoming participation by relatively reticent actors.[69]

I used a similar strategy to identify and recruit law enforcement respondents. I first drew a random sample of fifty-four agencies from the aforementioned California Department of Justice data set[70] and a random sample of California-based law enforcement agencies from a federal data set[71] for a combined sample of seventy-one agencies.[72] I estimated that seventy-one agencies would be sufficient to access at least five to seven agencies of different sizes and in different California counties.[73]

A comparison of the profiles of the twenty company staff[74] who participated in my research interviews with those of contactees who did

contacting people who worked at companies outside the sample, which permitted triangulation of the responses of the interview respondents recruited via random sampling. Using these methods, I secured twenty research interviews and eight triangulation interviews. See infra Tables 1 & 2.

[68] Mihail Plamenov Petkov & Lambros George Kaoullas, Overcoming Respondent Resistance at Elite Interviews Using an Intermediary, 16 Qualitative Rsch. 411, 418–24 (2016) (discussing the positive effect an intermediary has on rapport and the quality of information).

[69] Cf. Alex Marland & Anna Lennox Esselment, Negotiating with Gatekeepers to Get Interviews with Politicians: Qualitative Research Recruitment in a Digital Media Environment, 19 Qualitative Rsch. 685, 691 (2019) (describing alternatives to referrals to increase the effectiveness of interview outreach).

[70] State of California Department of Justice, supra note 65.

[71] Bureau of Just. Stats., U.S. Dep't of Just., Law Enforcement Agency Roster (LEAR), 2016 (Apr. 5, 2017), https://doi.org/10.3886/ICPSR36697.v1 [https://perma.cc/N2Q6-REWC].

[72] I started with a larger sample of police agencies (71) than of companies (54) because my professional network includes more people with connections to technology companies. Accordingly, I anticipated that I would conduct more cold outreach to investigators.

[73] For each of these agencies, I contacted the police chief or the sheriff to request permission to interview one or two investigators (random sampling). I also contacted people in my professional network who worked at prosecutors' offices and police departments in both the sampled agencies and agencies outside the sample (convenience sampling). When conducting interviews, I asked respondents if they would contact colleagues (snowball sampling). Using these methods, I secured twenty-seven research interviews and five triangulation interviews with enforcement agents and prosecutors. See infra Tables 1 & 3.

[74] Among the company research respondents, nine had frontline responsibilities, and nine had managerial roles, and two were outside counsel. See summary infra Tables 2 & 6.

not respond to recruitment outreach suggests that my sample is skewed toward respondents who worked for large companies with over 5,000 employees.[75] Among the company research respondents, six worked for companies with 500 to 5,000 employees, and twelve worked for companies with over 5,000 employees.[76] The larger organizational size, on average, of company respondents means that the people whom I interviewed likely processed larger volumes of compulsory legal process and interacted with a broader range of requesting agencies. These circumstances, combined with the fact that none of the respondents who participated in the study worked for telecommunications companies or internet providers,[77] means that my data better explain the practices of large companies, which typically offer a wider range of products and services.

A comparison of the characteristics of the agencies of the investigators[78] whom I interviewed with those of the agencies included in the random sample where an investigator was not interviewed suggests that my sample is skewed toward medium and larger police departments in metropolitan areas. The agencies of investigator respondents were larger than most departments in the United States—nearly half of which employ fewer than ten sworn officers and approximately 90% of which employ fewer than fifty.[79] All of the local and state agencies from which I interviewed an investigator had more than ten employees,[80] and only 33% of respondents worked at agencies employing fewer than fifty employees.[81] Existing research suggests that larger agencies tend to have officers with more specialization and training, and who participate in

[75] See infra Table 5.

[76] See id.

[77] While the original randomly drawn sample of 54 internet technology companies included several telecommunications companies and internet providers, none of the personnel employed at telecommunications companies or internet providers were among those who ultimately participated in the study.

[78] Among the investigator research respondents, fifteen were detectives, agents, or inspectors, while seven had supervisory roles. See summary infra Table 7. Five of the law enforcement research respondents were prosecutors: three were county prosecutors, and two were federal prosecutors. Id.

[79] Shelley S. Hyland & Elizabeth Davis, U.S. Dep't of Just., Local Police Departments, 2016: Personnel, at 3 (2019).

[80] See infra Table 5.

[81] Id. Eight law enforcement research respondents worked at agencies with fewer than fifty people, four worked at agencies with fifty-one to one hundred agents, eight worked at agencies with between 101 and 300 people, and four worked at agencies with more than 300 people. Id.

interagency task forces more often than smaller police departments.[82] My interview data, therefore, likely reflect the experiences of investigators who are, on average, more knowledgeable about how to use search warrants to obtain data from internet technology companies.

Given these limitations, my interview data are not of a suitable type or scale to permit the generalization of findings to all internet technology companies or to all law enforcement agencies. Nor are they of a kind that would enable us to precisely determine the prevalence of the experiences reported by respondents in my study among internet technology companies. However, the goal of qualitative research is rarely to make arguments about the representativeness of study findings. Instead, the aim of such research—including this Article—is to theorize mechanisms that explain the processes and experiences reported by research participants. As Part I suggests, the degree to which such mechanisms are at work likely varies by the breadth and variability of data types that companies have, the opacity of companies' data practices, and the subject matter of the case giving rise to the evidentiary demand.

C. Interviews and Analysis

Both the research and triangulation interviews were conducted between 2019 and 2023. For each interview, I used a semi-structured format, which involves both a planned set of questions and opportunities to discuss themes brought up during the research interviews.[83] My interview guide included questions asking respondents to discuss two recent examples of search warrants that they had either drafted or reviewed, with follow-up questions about their experiences with the warrant, such as, "Do questions arise when you are looking over a search warrant? Can you give me an example?" or "Do questions arise when you prepare a search warrant? Can you give me an example?"[84] This set of questions permitted

[82] Boustead, supra note 6, at 6. For large enough agencies, investigators typically constitute around 15% of the sworn staff in a police department or sheriff's office. Horvath et al., supra note 50, at 24.

[83] During both the research and triangulation interviews, I emphasized that interviewees could speak at a level of generality at which they felt comfortable and that I did not need to know any confidential or legally privileged details about their work. I also told participants that they could skip questions or ask me not to use particular parts of the interviews.

[84] During some interviews, respondents expressed concerns about discussing actual warrants that they had prepared or reviewed and responded using hypothetical examples rather than actual past warrants. For both sets of participants, I also asked about their career backgrounds, fields, interactions with others, work challenges, and changes in their work over

respondents to discuss their experiences at length and allowed me to follow up with questions about particular parts of their answers.[85]

During analysis, I coded the materials for both research and triangulation interviews iteratively, using standard qualitative approaches that moved between themes focused on law, technology, and organizations, and new themes and questions that emerged during the interviews and data analysis.[86] For the discussion below, I paraphrase, quote, and excerpt only from the forty-seven research interviews that I conducted. In each case, I have altered personal and organization-identifying information to protect research participants' confidentiality.

D. Company and Law Enforcement Perspectives

Existing research characterizes the approach that companies take in their evidence intermediary role as deliberate: companies are considered to either actively decide to resist government demands for evidence or actively try to help law enforcement. This characterization is borne out in some of the interview data. For example, some company respondents identified protecting users' data and privacy against government intrusion as a primary concern that animated their work.[87] Likewise, some company respondents emphasized a desire to assist law enforcement in obtaining evidence.[88] These respondents saw the production of evidence as part of broader company efforts to protect the safety of their users, including safety from physical harm and fraud.[89] The sense of serving a broader company- or community-wide effort to protect users from harm was particularly salient when respondents discussed cases involving

time. I concluded the interviews with background questions about participants' age, race, gender, education, department size, and organization.

[85] During each type of interview, I took shorthand notes and typed more detailed interview summaries afterward. For research interviews that were audio-recorded, the recordings were also transcribed.

[86] See Weiss, supra note 53, at 154–58 (describing the processes of coding and sorting interview data); Nicole M. Deterding & Mary C. Waters, Flexible Coding of In-Depth Interviews: A Twenty-First-Century Approach, 50 Socio. Methods & Rsch. 708, 722–33 (2018) (describing three main stages of coding and analysis).

[87] Interview with Legal Director 1 (Oct. 2021) (transcript on file with author); Interview with Legal Assistant 4 (Feb. 2022) (transcript on file with author).

[88] Interview with Safety Manager 1 (Oct. 2021) (transcript on file with author); Interview with Investigations Specialist 1 (Dec. 2021) (transcript on file with author).

[89] Interview with Product Manager 1 (July 2021) (transcript on file with author); Interview with Trust and Safety Lead 1 (Apr. 2022) (transcript on file with author).

investigations of child sexual exploitation, human trafficking, or potential suicide.[90]

More than cooperation or resistance, however, company respondents emphasized various practical difficulties that arose in their work. One set of concerns and constraints related to workload. For many respondents, the most salient problems associated with search warrants that sought large amounts of data or data from numerous categories was the amount of work—that is, the amount of human and technical resources—required to produce the responsive information. Some company respondents related withholding data called for by the warrant's language if the data fell outside the types or amounts that the respondents would routinely produce, especially if doing so would have required seeking additional engineering resources.[91] Likewise, respondents reported that a key downside risk of withholding responsive evidence was not necessarily the potential impact on officers' investigations but rather the possibility that it would cause an overall increase in their workload. For example, limiting data production to the extent that agents ceased to receive relevant information would increase the frequency with which agents followed up,[92] adding to the reviewer's workload and expanding the chances of government intrusion.

In addition to workload, company respondents reported problems identifying which categories of potentially producible company data fell within the language of a warrant. For example, the warrant's description of the desired data might read similarly to the following excerpt from a federal search warrant, which closely follows an exemplar in the 2009 U.S. Department of Justice Search and Seizure Manual ("DOJ Manual") for warrants to email service providers: "All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files."[93] The term "buddy list" came up in multiple interviews with company staff and law enforcement requesters. Some companies may not keep any information under the term "buddy list," while other companies might have one category of data termed "friends lists" and another category termed "buddy lists," creating

[90] Interview with Safety Manager 1, supra note 88; Interview with Investigations Specialist 1, supra note 88; Interview with Legal Director 2 (Mar. 2023) (notes on file with author).

[91] Interview with Legal Assistant 4, supra note 87.

[92] Id.

[93] H. Marshall Jarrett & Michael W. Bailie, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 261 (2009).

uncertainty as to which category the warrant sought.[94] An attorney for a platform-based rental company explained that he frequently reviewed search warrants that would speak of "session times."[95] Session times are data fields enumerated in section 2703 of the SCA,[96] referring to the time when users are logged onto an online service, such as a social media platform, and how long they remain on the service before logging off. The respondent, however, did not think that law enforcement wanted information about when and how long a user logged on to a specific application because his company was not a social media or communications provider but a company that facilitated rentals.[97] Thus, he would typically interpret this kind of "session" language as referring to information about when a user rented something and the duration of the rental.[98]

Company respondents also reported challenges interpreting two types of warrants: those that appeared to seek data about individuals and accounts potentially unconnected to the conduct being investigated and those that sought large volumes of data or data of numerous types about the individuals and accounts under investigation. Concerns about the first category of warrants arise when warrants ask for users' identities and accounts within a particular geographic area, as in the case of a geofence warrant, which identifies a particular geographic location and then asks a company to produce information about devices near that location.[99] They also arise when warrants ask the company to identify accounts that had been accessed during a specific period or that had accessed certain materials hosted by the company.[100]

Concerns about the latter category emerged when respondents discussed warrants that describe the data sought with a long list of data fields or that seek "all content," "all records," or data from "all" company products. Some company respondents discussed how broad "all" phrases

[94] E.g., Interview with Outside Counsel 4 (Mar. 2022) (notes on file with author); Interview with Sergeant 1 (May 2022) (notes on file with author); Interview with Detective 8 (Sept. 2022) (transcript on file with author).

[95] Interview with Counsel 4 (Mar. 2022) (notes on file with author).

[96] 18 U.S.C § 2703(c)(2)(C).

[97] Interview with Counsel 4, supra note 95.

[98] Id.

[99] Interview with Investigations Specialist 1, supra note 88. For an overview of geofence warrants, see Note, Geofence Warrants and the Fourth Amendment, 134 Harv. L. Rev. 2508, 2514–15 (2021).

[100] Interview with Legal Director 1, supra note 87.

were often meaningless because they could refer to any number of data categories, some of which could not be within the scope of a search warrant because they could not contemplate any investigatory usage for such data.[101] One reviewer discussed how the usage of the phrase reflected a lack of sufficient knowledge on the part of the officer and reviewing judge to evaluate the validity of a warrant:

> If a search warrant said, "we want all [company] information associated with [this email address]." What does it mean to turn over all [company] information? And if we do turn over all [company] information is that really within the spirit of what the search warrant should be? Or did this, like, 90-year-old judge sign it, not really knowing what it meant to get "all [company] information"?[102]

She described such warrants as overbroad because they failed to specify the exact categories of data that the investigator sought, which suggests that the investigator lacked probable cause to obtain data of all types falling under the "all" data demand. As she explained, warrants seeking "all" information, including from numerous company products, were "fishing" requests because those products likely "didn't form the basis for the warrant."[103] When I asked how she could tell that the agent did not know that these products were implicated when applying for the warrant, she explained that after receiving an "all data" demand, she would send the agent only some information associated with the account. Sometimes, the agent would then "follow up and say, 'Oh, actually based off of what you sent us, we now think that there's other information in these other products and services, so we want access to that as well.'"[104] To her, it was clear that those agents "didn't have that information on the front end, but they only came across that information after we gave them the first batch."[105]

With both such types of warrants, a reviewer may email or call the requester and attempt to figure out what the requester most needs.[106] One reviewer explained that he often sought "context" from agents about why

[101] E.g., Interview with Trust and Safety Director 1 (Apr. 2021) (transcript on file with author); Interview with Legal Assistant 4, supra note 87.

[102] Interview with Legal Assistant 4, supra note 87.

[103] Id.

[104] Id.

[105] Id.

[106] Interview with Trust and Safety Director 1, supra note 101; Interview with Legal Director 1, supra note 87.

they thought the company's users were involved.[107] Sometimes, an investigator would provide more information about the case, allowing reviewers to evaluate the seriousness of the case and brainstorm how they could narrow down the number of accounts or users identified and still achieve the requesting agent's goals. If the conversation did not feel "appropriate"—for example, if a reviewer sensed that agents did not know what they were seeking or that they were "fishing" for data—he would consider escalating the matter to a superior who would contact the requesting agent to better understand and narrow the request.[108] An attorney supervisor explained that one of her principal responsibilities was to handle "day-to-day escalations," which involved asking questions such as, "Is there sufficient probable cause articulated?"[109]

Law enforcement respondents reported analogous experiences: they did not encounter uniformly adversarial or uniformly cooperative attitudes on the part of company staff handling warrants. For example, many law enforcement respondents emphasized that companies could be very responsive, sometimes helping officers to identify what the company staff considered problems with the warrant directives and explaining how to draft language that would satisfy company reviewers.[110] One investigator explained that, after a reviewer rejected part of a geofence warrant that she prepared, she reviewed her warrant, but neither she nor a detective at another agency with experience drafting geofence warrants could figure out what was wrong with the request.[111] She then received an email and call from someone at the company, who explained that the physical address listed on the warrant did not match closely enough with the latitude and longitudinal coordinates listed on the warrant.

Other law enforcement respondents acknowledged that individual company reviewers often try to be helpful but expressed frustration that the companies, as organizations, respond to warrants in arbitrary and inconsistent ways. In particular, investigators reported being sympathetic to the workload faced by company staff, recognizing that gathering a large production would take longer than responding to a request that sought subscriber information alone.[112] Some respondents, however, commented

[107] Interview with Investigations Specialist 1, supra note 88.
[108] Id.
[109] Interview with Counsel 6 (Dec. 2021) (notes on file with author).
[110] E.g., Interview with Detective 4 (Apr. 2021) (transcript on file with author).
[111] Id.
[112] Interview with Sergeant 1, supra note 94.

that the time it took a company to respond sometimes seemed arbitrary.[113] One investigator quipped that some companies take a month to produce data "just because."[114] To him, the time taken by companies to respond did not always appear related to the type or volume of information sought in the warrant. Others reported that, when interacting with companies, their staff sometimes provided different answers on whether data can be produced.[115] Law enforcement respondents also reported analogous challenges in figuring out how to describe the data sought in a warrant in terms satisfactory to company legal compliance staff. For example, numerous law enforcement respondents emphasized that, both within and across companies, reviewers interpreted language in search warrants differently. Some explained that if he used a different term with the same or similar meaning, e.g., "friend list" instead of "buddy list," companies would respond that they did not hold the requested data.[116]

Other times, companies may provide rote responses to warrants, such as, "we cannot respond to your request" or "we have found no data," with or without explanation,[117] even though the investigator had other information suggesting that the data did exist. One investigator reported that he had a phone device on which his office undertook digital forensics and determined that photos were being backed up onto a cloud storage service.[118] However, when he sought data from that company, the company's attorney responded that no such data existed:

> [So] I get all of [the arrestee's] devices. We do forensics on all of his devices, [and] I go, "Hey, got a question for you guys [the company]. Your [production] said that there was nothing, but I have his phone. I see all of his photos. There's a lot here. And I go into his settings and his settings show they're being backed up to his [account]. So where are those photos?"

[113] Interview with Detective 9 (Sept. 2022) (transcript on file with author); Interview with Detective 8, supra note 94.

[114] Interview with Lieutenant 2 (Oct. 2022) (notes on file with author).

[115] E.g., Interview with Detective 3 (Mar. 2021) (transcript on file with author); Interview with Deputy Chief 1 (June 2022) (transcript on file with author); Interview with Commander 1 (Aug. 2022).

[116] Interview with Sergeant 1, supra note 94; Interview with Detective 8, supra note 94.

[117] E.g., Interview with Commander 1, supra note 115.

[118] Interview with Detective 10 (Sept. 2022) (transcript on file with author).

> [He recounts the company attorney's response:] "Our team says if they [the photos] were there, they would've produced it."[119]

The investigator described the attorney's response as confusing and suspicious because, as he put it, "They [the pictures] are there. I can see them. I have the devices. Why aren't they in the [production]?"[120] Other investigators reported similar experiences, particularly when they drafted a warrant using the same language as in the past but nevertheless received no data or different types of data from the company in return.[121]

Investigators also recounted instances of company reviewers trying to gain more information about the underlying investigation, including questioning whether the investigation had sufficient probable cause. One agent related an investigation in which company staff questioned whether he had sufficient grounds for seeking specific data.[122] He explained that "every single entity now poses some type of legal review," which, for him, meant that even after obtaining judicial approval of a warrant, he had to pass an additional review undertaken by companies:

> [S]o we go through the process and the judge is like there is probable cause, go do it—now we've got a company that's like, we don't think this is enough, we're not going to produce this information . . . [In that case, the company] were looking at some of the probable cause, and they were like, yeah, it probably happened. But we think you should get this additional information before we give you our information.[123]

Other investigators and prosecutors recounted similar experiences with companies questioning the sufficiency of facts justifying the warrant.[124]

Despite being aware of these problems, law enforcement reported infrequent follow-ups with companies to inquire about why certain data were produced or not produced. For example, when I asked officers if they asked company staff about missing or different data, they indicated

[119] Id.

[120] Id.

[121] Interview with Detective 3, supra note 115. One investigator reported receiving a type of data he had never seen before despite having used the same language in a previous warrant served to the company. When he asked the company to explain what these data were, he received no response. Interview with Detective 10, supra note 118.

[122] Interview with Agent 1 (Nov. 2019) (transcript on file with author).

[123] Id.; cf. Interview with Sergeant 2 (Sept. 2022) (transcript on file with author) (describing how companies fail to provide information to law enforcement despite court orders).

[124] Interview with Prosecutor 8 (Nov. 2022) (notes on file with author); Interview with Deputy Chief 1, supra note 115.

that they generally did not.[125] These responses were consistent with reports from company respondents.[126] As one director explained, "Every once in a while [law enforcement] will come back and they'll be like, 'I asked for friends list. You didn't give me friends list.' And then you're like, '[O]h, okay we'll do a one-off pull,' and then you do a one-off pull and you send [th]em their friends list."[127] Generally, however, law enforcement appears to follow up infrequently.

Collectively, my findings suggest that while company review staff are sensitive to the values of user privacy and safety, what happens when company employees execute search warrants is also shaped by a handful of recurring practical difficulties. For law enforcement, these problems concerned uncertainty about the nature, organization, and precise nomenclature of company data holdings and the opacity of companies' decision-making about what they produce. For companies, these problems arose when deciding what to produce in response to imprecise or impractically broad search warrant language without the benefit of specific information about the underlying investigation.

In many ways, these findings are poorly theorized in existing scholarship, which tends to conceive of internet technology companies as implementing unitary, deliberatively determined strategies of either cooperation or resistance.[128] However, the experiences reported by the respondents reflect not only intentional company priorities of privacy, safety, and efficiency, but also informational and communicative challenges arising from officers' drafting of warrants with language that company staff found too imprecise or impractical to comply with. Thus, while the intentional commitments of companies certainly play a role, existing scholarly accounts do not fully explain the nature of the problems that companies face nor the ways companies manage or respond to those problems. A different perspective is needed to understand contemporary third-party search procedure for internet evidence. The next Part develops such a theory.

[125] Interview with Detective 10, supra note 118; Interview with Sergeant 2, supra note 123; Interview with Prosecutor 8, supra note 124; Interview with Detective 6 (May 2022) (transcript on file with author); Interview with Detective 2 (Mar. 2021) (transcript on file with author).

[126] Interview with Counsel 2 (Sept. 2021) (transcript on file with author); Interview with Outside Counsel 4, supra note 94.

[127] Interview with Trust and Safety Director 1, supra note 101.

[128] See supra text accompanying note 11.

III. KNOWLEDGE MISALIGNMENT

In this Part, I develop the concept of "knowledge misalignment" to explain the predicaments that give rise to law enforcement agents being unable to draft search warrants with feasible and precisely described directives, and compliance staff finding themselves in need of often unavailable information about the underlying investigations to decide what information to produce. In Section III.A, I draw on organizational theory to define the concept of knowledge misalignment and to identify two types of misalignment: linguistic and substantive misalignment. In Sections III.B and III.C, I use the concept to explain the types of informational complications that companies encounter in responding to warrants, the practices that they have developed to manage them, and the ways law enforcement agents acquiesce to these practices.

A. Linguistic and Substantive Misalignment

Organizational theory provides several insights into how organizations interact with actors in their environment,[129] including how they learn to interact with actors with different values, priorities, and competencies. During these interactions, a basic tension that organizations encounter is whether to share information with outside actors and how much of it to share.[130]

On the one hand, organizations are prone to secrecy. Max Weber theorized that bureaucracy rests on "keeping secret its knowledge and intentions" from competing organizations and the public.[131] As Robert Merton put more concretely, "[c]ost figures, lists of clients, new technical processes, plans for production—all these are typically regarded as essential secrets of private economic bureaucracies which might be revealed if the bases of all decisions and policies had to be publicly defended."[132] Restricting information flow is thus a critical way for organizations to manage their relationships and dependencies on other organizations.[133]

[129] W. Richard Scott, Organizations: Rational, Natural, and Open Systems 8 (5th ed. 2003).
[130] Pfeffer & Salancik, supra note 31, at 45, 48, 53, 98, 105–06.
[131] 3 Max Weber, Economy and Society: An Outline of Interpretive Sociology 992 (Guenther Roth & Claus Wittich eds., 1968).
[132] Robert K. Merton, Social Theory and Social Structure 251 (1968) (describing "[b]ureaucratic structure and personality").
[133] Pfeffer & Salancik, supra note 31, at 45, 48, 53, 98, 105–06.

However, organizations must sometimes provide information to outside organizations and actors to successfully interact and build relationships with them.[134] Organizations may find themselves compelled by law to interact with certain other actors because, for example, a legal cause of action enables one party to sue another or a law requires an organization to produce information to other actors via compulsory legal process. When companies engage in these interactions, practical predicaments often arise because people have different organizational and occupational backgrounds and thus are part of disparate knowledge communities.[135] When these people communicate and interact, they tend to receive and filter information through the lenses of their organizations and their occupational communities. As a result, they may not fully understand or appreciate what others outside of their knowledge context are doing or saying.[136]

Building on these insights from organizational theory, I argue that a core type of problem faced by internet technology companies when processing compulsory legal process is the misaligned distribution of knowledge necessary for search procedure. Knowledge misalignment occurs when the distribution of necessary knowledge among individuals and organizations undertaking a joint task is misaligned with regard to the parts of the task for which each party is responsible.

In the context of search warrants for internet evidence, knowledge misalignment arises because warrant language is composed by investigators and prosecutors who are well acquainted with the facts of an investigation but have only limited knowledge of company data and operations. The task of executing the directives of those warrants, however, falls to company staff, who have organizational knowledge of company data and operations but often lack the information about the underlying investigation that they would need to reframe the warrant directive in a manner that is both efficient for the company to produce and sensitive to the investigation's needs.

The concept of knowledge misalignment is similar to that of information asymmetry in economics in that both are concerned with the

[134] Brian Uzzi, Embeddedness in the Making of Financial Capital: How Social Relations and Networks Benefit Firms Seeking Capital, 64 Am. Socio. Rev. 481, 483–84 (1999).

[135] Beth A. Bechky, Sharing Meaning Across Occupational Communities: The Transformation of Understanding on a Production Floor, 14 Org. Sci. 312, 312 (2003).

[136] Id. at 313.

difference in the information held by parties in a transaction.[137] However, the concept of knowledge misalignment is distinct in that it centers on differences between the knowledge that parties to a collective undertaking have and the knowledge that those parties would need to communicate with each other and perform their respective parts of the joint task.[138] In contrast, information asymmetry encompasses a broader range of transactional situations in which some information is better known to one party than to the other.

Knowledge misalignment is a core type of expertise problem that marks firm-state interactions in the era of informational capitalism. Julie Cohen has identified some of the informational problems that regulators now face: "Regulating information-era activities requires frameworks for making sense of the activities being regulated—for understanding how they work and identifying their legitimate and illegitimate modes of operation."[139] As she explains, the movement to informational capitalism "has disrupted many of the basic legibility rubrics that underlie and inform regulatory activity."[140] In particular, regulators largely lack tools to seek the kinds of disclosure that would enable meaningful oversight over companies' activities and systems, including those related to the operation of companies' data-driven algorithmic recommender and advertising systems.[141]

Compared to regulators, companies face a converse set of informational problems. When regulators seek information from companies, companies may not understand what the regulator is seeking or know what accompanying explanation they should provide to ensure that the regulator can make sense of the information.[142] These dynamics

[137] See Joseph E. Stiglitz, Information and the Change in the Paradigm in Economics, 92 Am. Econ. Rev. 460, 469 (2002). Knowledge misalignment is also distinct from Wendy Wagner's concept of comprehension asymmetries, which arise when one party—a speaker—has greater ability to understand or process information relevant to a communication as compared to the other party—the audience. Wagner, supra note 31, at 7, 13.

[138] See Bechky, supra note 135, at 313 (emphasizing that "even when knowledge is made explicit in a codified routine, when it is communicated across group boundaries, some organizational members may not understand it because they apply and interpret this knowledge within different contexts").

[139] Cohen, supra note 12, at 173.

[140] Id.

[141] Id. at 179–80.

[142] Ruthanne Huising & Susan S. Silbey, Governing the Gap: Forging Safe Science Through Relational Regulation, 5 Regul. & Governance 14, 16 (2011); Garry C. Gray & Susan S. Silbey, Governing Inside the Organization: Interpreting Regulation and Compliance, 120 Am. J. Socio. 96, 99 (2014).

emerge in the context of third-party search warrants partly because internet technology companies often keep secret information about the data that they collect and the ways they use it.[143] This leaves organizational outsiders—including legal actors seeking evidence—with relatively little knowledge about what exact types of data companies hold, for how long they hold it, or how easy or difficult it is to find and produce such data.

This set of circumstances collectively leads to two types of knowledge misalignment: linguistic and substantive misalignment. A *linguistic misalignment* arises when company staff encounter search warrants directing them to produce data described in terms that do not align with the company's own terminology for referring to the data that it holds. Such misalignment occurs because the core work of investigators involves discovering facts about what happened, who was involved, and whether those persons committed criminal offenses. Prosecutors, in particular, are focused on the specific elements of formal law, trying to link particular facts and evidence to legal elements to determine whether criminal offenses have been proven. As a result, law enforcement often drafts compulsory legal demands with investigatory and litigation goals in mind but without a thorough knowledge of or focus on companies' products or data holdings.

A substantive misalignment arises when company staff reframe search warrant directives into tasks manageable within the constraints of the company's dedicated resources and tractable with respect to familiar routines. Company reviewers often undertake this task with little knowledge of the circumstances of the investigation because they do not receive information about the substance of the underlying case. A search warrant application typically contains two components: a proposed warrant describing the persons, places, or objects to be searched and the items or "things" to be seized, and an affidavit explaining the experience and background of the officers and the evidence giving rise to probable cause that the contemplated search will yield evidence of a crime.[144] Technology companies, however, generally do not receive a copy of the

[143] See supra Subsection I.B.3.

[144] The police investigator or prosecutor typically prepares both documents and submits both parts to a judge for review. Van Duizend et al., supra note 51, at 1. If a judge finds that the agent's affidavit demonstrates "probable cause" and that the warrant enumerates which spaces and persons can be searched with sufficient "particularity," the judge can issue the warrant. See U.S. Const. amend. IV.

affidavit describing the factual circumstances of the case when they receive a search warrant. They typically receive only the warrant listing the items to be seized, the statute or formal law under which the warrant was issued, and the offenses under investigation. Because companies typically do not receive a copy of the affidavit, they know little about the substantive facts underlying a case beyond what they might infer from the list of statutes in the warrant.

Accordingly, when companies review a search warrant, they read the document with an eye toward a different set of knowledge and concerns: questions about how the description of the data sought in the warrant is supposed to line up with the actual categories of data that their company has, and concerns regarding the technical and organizational costs and risks that the task called for by the compulsory process will involve. As third parties not directly involved with the activities or people in a dispute or under investigation, companies have little independent reason to interact with an evidence seeker beyond the legal obligation of formal process. Nor do they presently have any legal obligation to informally consult with evidence seekers to assist them in framing the language of compulsory evidence demands.

Both forms of knowledge misalignment are amplified by the number and variety of law enforcement agencies in the United States, which include investigators and prosecutors at the 18,000 or so federal, state, and local law enforcement agencies in the country.[145] The language used in warrants can vary among these numerous agencies. Consider this language from a search warrant that a local police department in California served to a social media company:

> User content (e.g., photos, comments, videos, direct messages, and other materials) posted by the user to Instagram / Facebook. Sent, received and stored messages associated with the user account.
>
> Friend's lists with usernames[.][146]

Whereas many federal search warrants may closely follow model language suggested in the DOJ Manual, language used in local warrants,

[145] Duren Banks, Joshua Hendrix, Matthew Hickman & Tracey Kyckelhahn, U.S. Dep't of Just., National Sources of Law Enforcement Employment Data 1 (Oct. 4, 2016), https://bjs.ojp.gov/content/pub/pdf/nsleed.pdf [https://perma.cc/B87S-DD93].

[146] Search Warrant Served on Facebook Inc. and Instagram LLC, Cal. Super. Ct. Alameda Cnty., Report No: 19-050544, at 1 (obtained from Superior Court of California, County of Alameda) (on file with author).

subpoenas, and court orders likely varies more widely. Indeed, for many of the local law enforcement officers whom I interviewed, figuring out how to describe the data sought in a warrant in terms satisfactory to company legal compliance staff was a challenge. One detective emphasized that with many companies, products, and terms that change from "one place to another," it is "hard to draft language."[147] Another investigator shared a similar view: "[W]e try to be as specific as possible, but the data points change from each of the different services. So there is some generalit[y], so [its] username or whatever designation that might be handle or something like that."[148] The variety of agencies means that companies have to deal with many agencies and differing language used by those agencies.

The consequences of linguistic and substantive misalignment are exacerbated by agency rotation practices for local law enforcement investigators. Several respondents reported that police investigators typically work for between two and four years in their role before being moved out of the position to another role, often back to patrol.[149] The purpose of the rotation is to enable officers to gain a broader range of experience through work on investigations, which they can also bring back to their work in patrol. Several respondents emphasized that it could take years for officers to gain competency and expertise in investigative work involving internet and digital evidence, depending on how often they prepare warrants.[150] However, after gaining expertise, they are often rotated back into a non-investigative role,[151] which may cause substantial losses in expertise for an agency.

B. Managing Misalignment

With an understanding of knowledge misalignment, we also gain insight into the ways in which companies respond to search warrants. These processes include four methods for managing linguistic and substantive misalignment: company compliance staff's *acquisition* of

[147] Interview with Sergeant 1, supra note 94.

[148] Interview with Agent 1, supra note 122.

[149] E.g., Interview with Sergeant 1, supra note 94.

[150] E.g., Interview with Detective 10, supra note 118; Interview with Detective 11 (Oct. 2022) (transcript on file with author); Interview with Lieutenant 1 (July 2022) (transcript on file with author).

[151] E.g., Interview with Sergeant 1, supra note 94; Interview with Detective 10, supra note 118.

information about the data being sought and the case giving rise to the search warrant, *reconstruction* of language in the warrant into the company's nomenclature for the data in its possession that compliance staff believe to be relevant, *standardization* of data production, and *insulation* of company knowledge.

1. Acquisition

A core way that companies manage substantive and linguistic misalignment is to directly acquire information that they lack from the officers seeking evidence. Company respondents discussed how they clarified questions about the language and substance of cases through ad hoc conversations and more systematic mechanisms. On an individual basis, for example, company respondents may email or call an agent to clarify precisely what categories of data the officer sought by asking her, for example, to explain what she had in mind in using terms like "buddy lists" or "session times" in the search warrant.[152]

A more systematic way that companies try to gather information about demands is to collect it via web pages. Some companies have created web pages or law enforcement "portals" to permit law enforcement agents to submit legal process requests.[153] These web pages may be developed internally or purchased from outside vendors.[154] Some portals are simple intake forms that request information from an agent—such as her badge number and agency name—and allow her to upload a PDF copy of the legal process.[155] Others are more complex, requiring agents to register for an account using an official agency email before they can submit a request.[156] Submitting a demand via these portals may require that agents complete a series of pages asking for information about the request, including information beyond what is contained in the uploaded copy of the legal process.[157]

[152] See supra Section I.C.

[153] See Kerr, supra note 9, at 769.

[154] Interview with Outside Counsel 4, supra note 94; Interview with Safety Manager 1, supra note 88; Interview with Trust and Safety Lead 1, supra note 89.

[155] E.g., Legal Request Submissions, Twitter, https://legalrequests.twitter.com/forms/landing_disclaimer [https://perma.cc/85SJ-Y9D4] (last visited Apr. 8, 2024).

[156] See Kerr, supra note 9, at 769 ("Several portals have public-facing pages, although a government e-mail address is needed to set up an account.").

[157] E.g., LE Portal User Guide, Uber (Dec. 30, 2019), https://uber4.my.salesforce.com/sfc/p/#36000000j7x3/a/0e0000009NsJ/RI7vYMqLQcKXQoqzzFRNhSWPULyD6dewZpcsypBXXGI [https://perma.cc/84HC-93KE].

These web pages were reported to be important tools for reducing factual and language questions. When agents are tasked with inputting data via portals, fewer interpretive questions arise because agents may have to select from a "menu" of data types sought in the warrant or input information about the crime that they are investigating.[158] By collecting basic facts about a case, such as whether it involves child exploitation, assault, or fraud, companies can also gain greater perspective on the substance of the case and the types of data that would be relevant and responsive to it.[159]

2. Reconstruction

Another way that company reviewers manage misalignment is to reconstruct the demand or to imagine the types of data most likely to be relevant to law enforcement. This process can involve providing substantially less data than that explicitly sought in a warrant or producing data of a different type than that being demanded. It often happens in response to requests that seek "all records" regarding an account.

As one attorney explained, companies "self-narrow" by "defin[ing] for themselves what 'all data' means."[160] Consider this example of warrant language, which again follows the sample provided in the DOJ Manual:

> *All records or other information* regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).[161]

[158] Id.; see also Interview with Sergeant 1, supra note 94.

[159] Interview with Legal Director 2, supra note 90.

[160] Interview with Outside Counsel 4, supra note 94.

[161] United States v. Bickle, No. 10-cr-00565, 2011 WL 3798225, at *14 (D. Nev. July 21, 2011) (emphasis added); In re Target Email Accounts / Skype Accounts, Nos. 13-mj-08163, 13-mj-08164, 13-mj-08165, 13-mj-08166, 13-mj-08167, 2013 WL 4647554, at *1 (D. Kan. Aug. 27, 2013) (same); see also In re Search of Info. Associated with [redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 3 (D.D.C.), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014) ("All records or other information stored by an individual

As many interviewees described, when company reviewers encounter language in warrants seeking "all records," "all information," or the like, they decide what to produce by making their own more-or-less educated guess about what would be relevant to the requesting officer's investigation. To do this, the reviewer tries to imagine what the investigation is about and what, within the company's data, would be relevant to such an investigation. The reviewer then assembles and produces a subset of the data called for by the warrant's language, limited to those types of data that the company regularly produces *and* that would be relevant to the investigation *as the reviewer imagines it*. This response from a director exemplifies this perspective:

> [E]very Silicon Valley company has more data than they actually provide in search warrants . . . . [But] does it really matter? No. Does law enforcement ever care that you click "like"[?] . . . . [T]hey care about the content, they care about the interactions. . . . [But] [t]hey don't care that . . . you tried to upgrade three times.[162]

Other company respondents related a similar process of imagining the needs of an investigation and limiting their production accordingly.[163]

Some respondents at companies with large numbers of products reported that, in response to warrants requesting the production of "all data," they may provide only data for the one or two paradigmatic products most associated with the company.[164] As one reviewer explained,

> [S]ometimes the language . . . [sought] pretty much anything . . . related to this user. . . . [W]e're sitting there like, now you get the standard, here's the username, here's the login logouts, and because you said [email], we will give you th[e] mailbox. [But if you wanted any information about other products he might have used,] [n]o. . . . [Y]ou have to actually explicitly state that's the data set that you want . . . .[165]

using each account, including address books, contact and buddy lists, pictures, and files . . . .").

[162] Interview with Trust and Safety Director 1, supra note 101.

[163] Interview with Counsel 4, supra note 95.

[164] Interview with Trust and Safety Director 1, supra note 101; Interview with Legal Assistant 4, supra note 87; Interview with Outside Counsel 4, supra note 94.

[165] Interview with Legal Assistant 6 (Sept. 2021) (transcript on file with author).

Without factual context about a case or further details about what law enforcement has in mind when seeking "all data," reviewers make a best guess at the information most likely to be relevant.

Company reviewers also emphasized that they narrowed search productions by restricting the dates for which data were sought.[166] As some respondents explained, if they received a request asking for hundreds of accounts, they would try to have a conversation with the requester to see if the request could be narrowed, for example, by reducing the date range.[167] Law enforcement reported similar experiences. One investigator gave an example of an investigation in which he sought data covering approximately two months to identify patterns in behavior.[168] Such a period of data would allow him to obtain a sense of the places that the subject frequents, where they sleep at night, and when they are home.[169] However, the company uses shorter date spans for no clear reason.

3. Standardization

Companies invest substantial labor in deciding which of their internal data should be treated as corresponding to terms frequently used in the warrants that they receive.[170] Over time, they try to standardize their interpretations and reconstructions by institutionalizing decisions in policies and guidance for staff.[171] Several company respondents referred to guidance and training materials for mapping search warrant language onto particular products and data, which they described in terms ranging from playbooks, to charts, to slide decks.[172] Guidance documents of this kind might, for example, set forth the various types of data accessible for particular products and services. As one reviewer explained, a "granular understanding" of how company products work is critical to knowing how to appropriately respond to warrants.[173]

[166] Interview with Trust and Safety Director 1, supra note 101.

[167] Interview with Investigations Specialist 1, supra note 88; Interview with Trust and Safety Director 1, supra note 101; Interview with Legal Director 1, supra note 87.

[168] Interview with Sergeant 2, supra note 123.

[169] Id.

[170] See supra Sections II.D & III.A.

[171] See Interview with Safety Manager 1, supra note 88.

[172] Interview with Outside Counsel 3 (Nov. 2021) (transcript on file with author); Interview with Legal Assistant 4, supra note 87; Interview with Safety Manager 1, supra note 88; Interview with Outside Counsel 4, supra note 94.

[173] Interview with Counsel 6, supra note 109.

Such training materials, however, may be outdated or disorganized. For example, one respondent reported that company product teams would change particular services and data flows without notifying the law enforcement response team of changes to the capabilities of their query tools or the arrangement of product databases.[174] Thus, company compliance staff sometimes do not know if a previously inaccessible type of data has been made accessible to them or if data that the company has previously produced have ceased to be accessible.

To varying degrees, companies also try to facilitate officers' use of standardized language in their warrants by publishing law enforcement guides.[175] These guides are often publicly accessible on company websites and provide basic information about the company, its products and services, and its policies for responding to compulsory legal process. Apple's guide, for example, lists and explains the company's numerous products and services and offers some general guidance on the types of data that those products and services gather.[176] That guide also includes an effort to explain what data are unavailable and provides basic descriptions of the types of data not accessible to the company due to encryption.[177]

The interview data suggest that promulgating guides specifying the exact language that police should use to request particular types of data is a means by which many internet technology companies reduce the linguistic misalignment encountered by company staff. Investigators discussed the importance of these guides for choosing how to word the descriptions of the types of data sought in their warrants.[178] One sergeant described company guides as instructions for the language the company would like to see in a warrant.[179] Another investigator similarly regarded the guides as instructions on the exact words that the company expected him to use if the company was to produce the data that he expected to receive:

[174] Interview with Trust and Safety Director 1, supra note 101.

[175] Interview with Outside Counsel 3, supra note 172; Interview with Outside Counsel 4, supra note 94.

[176] Apple, Legal Process Guidelines: Government & Law Enforcement Within the United States 3, 7–19 (June 2024), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/7YUD-WXGU].

[177] Id. at 12–14, 16.

[178] See Interview with Lieutenant 1, supra note 150; Interview with Detective 8, supra note 94.

[179] Interview with Sergeant 1, supra note 94.

> Interviewer: Earlier, you mentioned that companies have different names for [usernames and handles]. How do you keep up with the names of—even just what information, and how they call it?
>
> Respondent: A lot of times, that was the law enforcement guide. We'll use some of that terminology from either an old law enforcement guide, or, maybe, somebody else that's run into a problem where a company refused to provide the information because we weren't calling it the right thing—we don't have any usernames. We're, all, I don't know screen names. Okay, just tell me what to write down . . . I loved it. . . . [But] . . . tell me exactly what you expect. I do that within my reasonable power to do so. And I get exactly what I expect. This is perfect, nice, regimented, organized. I loved it.[180]

Law enforcement portals similarly instruct officers about the data that companies hold and the language that companies use to describe those data, sometimes by way of links to information about the company or by requiring officers submitting warrants through the portal to click through pages displaying menus of company data types and prompting officers to select from them. One officer explained that she finds company portals quite useful in determining what data to request when drafting search warrants:

> [This company] is really helpful in that they have a support link on the online portal that will tell you, "[F]or [this product], this is all the information that we keep that you can ask for. We don't keep this, this or this." So you can reference that as you're writing your search warrant and be like, okay, of all the information they do keep, this is the information that I want and [I] just list it out.[181]

Finally, companies also standardize interpretations and reconstructions among staff through the capabilities of the software tools that they create for compliance staff to systematically query company databases. A sophisticated query tool may enable staff to search and extract data from one or more databases according to whatever parameters are programmed into the tool. The main alternative—manually opening, navigating, and copying selected portions from individual data tables—is sometimes feasible, depending on the size and complexity of the databases and the

[180] Interview with Agent 1, supra note 122.
[181] Interview with Detective 3, supra note 115.

parameters of the request. However, manual pulls prove more challenging for staff—usually at larger companies—who handle large volumes of requests. Larger companies that receive more requests may allocate engineering staff time to creating basic web pages or writing common queries that law enforcement response staff can use to pull data repeatedly.[182] Multiple reviewers explained that pulling data involved going to product-specific web pages with crude data export options, which they could then "press" to download data.[183] Over time, some reviewers learned to write basic structured query language to pull data from the backend data tables associated with products.[184]

Larger companies sometimes also develop more automated tools capable of pulling data from various products. Such a tool may also reduce the time required to produce data relative to that needed for what one reviewer described as an export-standardize-format process.[185] One lead reviewer explained that when pulling requests was primarily manual, it might take thirty minutes to query and export a record, standardize the data, and then put it in a spreadsheet or other commonly used format to send to the agent.[186]

When companies build a querying tool, the tool institutionalizes what reviewers have understood and imagined to be relevant to law enforcement. For example, a director explained that when he worked on building the tool for his company, he thought a great deal about the types of data that law enforcement would *expect* to see in an account:

> [W]hat I'm trying to do is create a package and this package . . . needs to fulfill all of the *expectations* of what . . . law enforcement *thinks is in the account*, and hopefully it is also going to fulfill what is necessary to do the investigation.[187]

He continued:

> [E]ffectively you are doing an exercise of what are the pieces of data that law enforcement *is likely to care about* and how do we do that easily? And then again, most user-generated content will fall under this.

[182] See Interview with Engineer 1 (July 2021) (transcript on file with author).

[183] E.g., Interview with Legal Assistant 4, supra note 87; Interview with Trust and Safety Director 1, supra note 101.

[184] E.g., Interview with Legal Assistant 6, supra note 165.

[185] Interview with Investigations Specialist 1, supra note 88.

[186] Id.

[187] Interview with Trust and Safety Director 1, supra note 101 (emphases added).

> So it's not like . . . I'm going to hide data from law enforcement. Obviously that's not acceptable.[188]

Once a tool is created, whatever data fields company staff imagined to be important to officers who request data of that type come to be institutionalized as the search parameters available to future staff using the tool. This director further explained that, once his company's internal engineering team developed a tool that allowed his staff to search particular databases, staff members would use that tool to provide a standard set of information, even if the warrant asked for different data:

> [N]ow you have a tool and effectively for the next probably year, year and a half, two years, depending on what your scale is, you literally do not touch that tool. . . .
>
> [E]very time someone's [here with a search request], you click the button in the tool, it spits out a file and then you send them that file.[189]

Company staff respondents recognized that infrequent revisions to and maintenance of tools can lead to problems. The director commented that a query tool could break down because new product features were added or backend data tables had been changed and no one had informed the law enforcement response team.[190] At times, the tool could produce incorrect or incomplete data—requiring manual reviews and data pulls. He commented that he sometimes would not know that a tool had failed to produce data until a recipient reached out to say that the expected data were not in the production.[191]

4. Insulation

While many of the above practices tend to reduce knowledge misalignment between evidence seekers and company reviewers, they can also create and reinforce misalignment. For example, law enforcement portals and guides disseminate information about certain types of company data and the company's internal nomenclature for those data. While such tools facilitate the work of requesting, searching, and producing the types of data that the company has selected for inclusion in the portal or guide, they omit knowledge about other data types. In other

[188] Id. (emphasis added).
[189] Id.
[190] See id.; Interview with Engineer 1, supra note 182.
[191] Interview with Trust and Safety Director 1, supra note 101.

words, if companies do not offer a ready option to select a particular type of data or do not discuss a particular type of data in their law enforcement guides, the existence of the omitted data type is obscured, along with the terminology with which an officer could frame a request for it that company staff would recognize.

Data types might be omitted simply because such data are new and the portal or guide has not been updated, or because the company has not developed the query tools that staff would need to produce them. There are likely also many types of data that company staff do not think could ever be relevant to a police investigation and whose inclusion staff believe would only clutter the company's guides and portal menus with information about data types that will seldom, if ever, be of any actual use to the police. In other instances, company staff might realize that a type of data is potentially valuable for a wide enough range of cases that officers, once aware of it, will request it in their warrants as a matter of routine, adding substantially to the workload of compliance staff. Although officers may well come to know of the existence of an omitted data type and can include a request for it in a search warrant, their efforts are more likely to be misunderstood or ignored by the company staff processing the warrant,[192] such that getting the data produced will be possible, if at all, only by way of following up and directly communicating with the staff handling the warrant.

Portals and guidelines can also reduce the need for the types of direct and informal communication between requesting agents and company staff through which knowledge misalignment can be resolved on an ad hoc basis. Some company respondents, both in-house and outside counsel, expressed concerns about compliance staff revealing too much information to law enforcement about the data held by companies and about companies' internal policies for interpreting the language in compulsory requests.[193] One respondent emphasized that a good part of their work consists of navigating when and how much to explain company data to officers.[194]

Once a portal or guideline has obviated the need for direct communications between officers and compliance staff with respect to the company's most frequently sought types of data, it becomes feasible for

[192] See Interview with Deputy Chief 1, supra note 115.

[193] See Interview with Legal Director 1, supra note 87; Interview with Outside Counsel 4, supra note 94.

[194] Interview with Investigations Specialist 1, supra note 88.

company decision makers to prevent such conversations altogether. As one detective reported, this leaves officers with little recourse when something has gone wrong with one of their more standard data requests, as is inevitable in the volume processing of hundreds of warrants in a company staffed by human beings:

> And so I think that's one of the biggest deficits right now is [that at] a lot of these companies trying to talk to a human is next to impossible. They will not let you talk to people. They will have one representative . . . that law enforcement can deal with. Everything else is through a portal. I've gotten one call from someone doing legal process. [Bec]ause they need clarification, but they cannot provide you with their email [or] phone number. You don't contact them, they contact you. And so you're kind of left just wondering on a lot of stuff . . . . I asked for this and it's normally provided, I asked for it here, [but] it's not in [the production]. So does that just mean they don't have it? Or does that mean it was left out?[195]

Cutting off direct, staff-to-officer communications about data production can also close off the main means by which misalignment concerning the types of data *omitted* from the portal or guide might be resolved. In this way, these techniques also tend to preserve misalignment that bolsters the company's de facto prerogative to withhold particular parts of its data holdings from the universe of data accessible to legal actors through compulsory process.

In a similar manner, companies may discourage staff reviewers from alleviating knowledge misalignment that is convenient to the company by providing staff with template responses to law enforcement demands. One lawyer, who serves as outside counsel to technology firms, explained that template responses help to contain the range of responses that company staff—many of whom are not lawyers—might provide.[196] The interview data suggest that, while some companies—and some staff within companies—have informal phone calls and emails with investigators, others do not, or have them much less frequently.[197] The effect of this insulation may be to preserve, for more senior company decision-makers, the ability to decide when, and whether, to dispel knowledge

[195] Interview with Detective 10, supra note 118.
[196] Interview with Outside Counsel 4, supra note 94.
[197] See supra Section II.D; see also Interview with Lieutenant 1, supra note 150.

misalignment that impedes or prevents law enforcement from accessing particular parts of the company's data holdings.

C. Acquiescing to Company Management

The concept of knowledge misalignment also helps us understand how law enforcement responds to inconsistency and arbitrariness in company responses. As the above analysis suggests, internet technology companies appear, on the whole, to have created teams, systems, and processes that allow them to manage the scale and scope of their search warrant obligations and the informational and communication problems that arise with those obligations. Across all the law enforcement agents whom I interviewed, not one reported glaring problems with their work or interactions with company reviewers.

A big reason for this is that companies' management practices may very well lead to a data production more useful to law enforcement compared to an assiduous production of all the material called for by a literal construal of the warrant language. For example, when companies narrow their productions in response to warrants seeking "all records" associated with an account or a transaction, company staff tend to decide what to produce based on a more-or-less educated guess about what data would be relevant.[198] They produce data, for example, for only the paradigmatic products associated with the company or for data categories within an established subset or "menu" of data.[199] Because these guesses are often shaped by staff's experience reviewing warrants,[200] the evidence produced after company-initiated narrowing may be better tailored to the officer's investigation needs than the entire mass of evidence called for by the warrant's language. Without company efforts to reconstruct the meaning of warrant language that poorly aligns with the companies' products and data holdings, companies might well end up expending more resources to provide law enforcement with large and confusing data productions in which the material that the officer really needs is either buried or not included at all.

At the same time, the interview data suggest that the techniques that companies have developed to respond to compulsory legal process are ultimately still makeshift in operation: these methods are expedient and

[198] See supra Subsection III.B.2.
[199] See supra Subsections III.B.1 & III.B.2.
[200] See supra Subsection III.B.2.

generally functional, but they can lead to overproduction, underproduction, and inconsistent production of data across demands. In many cases, companies may produce less than the data listed in a warrant. In other cases, they may produce more, or simply different, data than what is called for in the warrant.

Recall the discussion of how companies reconstruct search warrant language to align the data produced with what company reviewers believe the requesting officer had in mind when authoring the warrant. One reviewer, for example, reconstructed search warrants seeking "session times" to fit the types of records that his company would have in its possession.[201] Another reviewer emphasized that if a warrant sought basic subscriber information about a customer, the company would not provide information about the subscriber's upgrade history as part of the production because that was not a type of information that he believed to be relevant to law enforcement.[202] When the company undertakes these reconstructions, the investigator receives only what the reviewers decided fell within their determination of what law enforcement had in mind when requesting the data, usually without notice that the company has withheld responsive data.

Companies also over- or underproduce data as a matter of technical expedience. Recall one director's account above of how tools are created and left unchanged for periods of time.[203] He emphasized that, once a tool allows staff to search particular databases and produce certain types of data, staff use that tool to provide a standard set of information, even if the warrant seeks different data.[204] Over time, the data produced in response to warrants becomes tied less tightly to the content of the warrant than to the existing functionality of the querying tool or the data fields available for officers to select from on the portal. Through both companies' reconstruction of the terminology and investigative context of search warrants and standardization of those interpretations in the technical functions of intake portals and querying tools, which data are produced in response to search warrants becomes less a matter of what is called for in the judicially approved written demand and more a matter of what data the company can quickly and conveniently pull. These efforts

[201] See supra text accompanying notes 96–98.
[202] See supra text accompanying note 162.
[203] See supra Subsection III.B.3.
[204] Id.

can result in companies simultaneously producing less *and* more data than what a warrant calls for.

Several law enforcement respondents reported receiving data not explicitly sought in their search warrants. One investigator explained that, when drafting search warrants, he sets a date range but routinely receives data beyond what was requested.[205] Such errors may result from companies rearranging where various data types can be found among the backend tables without notifying the teams reviewing compulsory legal process.[206] One respondent commented that he finds, on occasion, that the data pulled by a query do not match the actual data that he sees on his computer interface.[207] He explained that, when data systems are modified, their team is often not notified, leaving them unaware of problems in their data production unless they double-check the output of the querying tools or investigators report that those data are missing from productions.[208]

Law enforcement often does not notice these irregularities because they do not know exactly what data companies have, how companies interpret their warrant, or what data companies choose not to produce.[209] When law enforcement does notice production problems, it is often because a company has failed to produce data known to exist.[210] Even then, law enforcement investigators generally appear to acquiesce to company practices.[211]

The interview data suggest that investigators acquiesce to company practices for two sets of reasons. First, investigators and prosecutors are constrained in time and resources. If they obtain some usable evidence and are unsure whether the company can or would produce additional evidence, they are unlikely to spend time asking follow-up questions and are even less likely to litigate the issue. This response from an experienced agent is typical of many responses offered by law enforcement officers who reported being resigned to accepting company practices:

[205] E.g., Interview with Prosecutor 8, supra note 124. These types of errors have also been noted in judicial opinions. United States v. Bickle, No. 10-cr-00565, 2011 WL 3798225, at *8 (D. Nev. July 21, 2011) ("Mr. Damm also explained that the warrant only sought email communications beginning March 2009, through the date of the application. However, Microsoft sent a disk containing emails dating back to April 2006.").

[206] Interview with Trust and Safety Director 1, supra note 101.

[207] Id.

[208] Id.

[209] See supra Subsection III.B.4.

[210] See supra Section II.D.

[211] Id.

> So when these companies say, "We don't have them," what they mean is, "We don't have them in a way that is really easy to access and there's no real guidelines in the law in terms of exactly what we have to do. And [we, the company, are] making a sort of calculated effort, a calculated guess, that you're not going to sue us too hard over this." And because no one knows exactly how it's going to come out . . . [the] company might say, "We cannot provide you with this or that piece of information . . . ."
>
> And then the authorities are left with, "Okay, do we now stop what we're doing long enough to try to find the technical expertise to convene a bunch of lawyers and technologists, presumably from federal partners because they're the ones that are going to have the best resources and really take a deep dive in a show-cause hearing against a very well-resourced company where the referee is going to have to be a judge that doesn't entirely understand this complex issue and where the local prosecutor who is trying to keep up with a docket of violent crime and sexual assault . . . [says], 'Wait. . . . You want me to take a month to fight a giant company that has a jet full of really sophisticated lawyers that they're going to send? Is that the best way to spend our resources?'"And often, the answer is "No." Right? So that's why some of these issues aren't really fully explored despite the fact that there would be a public safety benefit to exploring them.[212]

The agent's response reflects a strong awareness that the company is withholding data falling within the scope of the search warrant. However, similar to other law enforcement respondents, he does not challenge the company because he does not believe that litigating such matters would be a good allocation of public resources. In particular, he does not believe that he or prosecutors would have the capacity to explain the circumstances in such a way that a generalist judge, lacking expertise in company products, architecture, and processes, would be persuaded. Accordingly, he accepts the company's determination of what will and will not be produced.

In addition to time and resource constraints, investigators expressed concerns about what company staff would think about their competence and how staff might deprioritize their warrants if they perceived officers to be incompetent or bothersome. One officer expressed concerns about

[212] Interview with Deputy Chief 1, supra note 115.

falling from the good graces of company staff by following up too often or following up on requests for less urgent cases.[213] Another reported that when they did get a phone number, they used that number sparingly because they were sensitive to how many calls that person must receive.[214] When agents discussed instances in which they did follow up with a company, they typically involved investigations deemed urgent, such as a series of arsons,[215] or cases in which the agency knew—from discussions with colleagues or from a previous production—that the company had previously produced data of the type omitted.[216]

Thus, the interview data suggest the existence of law enforcement acquiescence to company practices. Company staff, faced with substantive and linguistic misalignment, make ad hoc decisions about what data to produce and not produce, shaped, in part, by their own guesswork about what is needed for various kinds of police investigations. These decisions develop into practices for dealing with recurring misalignment, which are sometimes institutionalized in query tools and company guidance documents, and company decisions about what information to share in guidance and portal menus. The reasoning behind company decisions, with their consequences for what data are included in or withheld from data productions, goes on behind closed doors and largely unknown to officials who lack detailed knowledge of the companies' exact organizational rules, procedures, and technical capacities, be they the law enforcement investigators who request evidence or the prosecutors who would use it in court. However, because companies produce some data that is, often enough, useable, resource-constrained investigators and prosecutors lacking expertise in company data holdings generally accept companies' processes and procedures, making do with what data they receive.

IV. IMPLICATIONS FOR SEARCH PROCEDURE

Thus far, this Article has sought to explain the types of knowledge misalignment that shape third-party execution of search warrants seeking internet evidence and the practices that companies employ to manage such misalignment and, in some cases, selectively preserve it. This Part

[213] Interview with Detective 2, supra note 125.
[214] Interview with Agent 1, supra note 122.
[215] Interview with Detective 4, supra note 110.
[216] See supra text accompanying notes 117–21, 125–27.

identifies potential institutional consequences of companies' practices—and law enforcement agents' corresponding acquiescence to them—for search procedure.

Section IV.A discusses the potential untethering of evidence production from the procedures of the Fourth Amendment currently underway as companies determine the scope of actual searches with reference to the criteria and procedures that the companies have internally developed to cope with knowledge misalignment, which tend to favor producing routinely supplied data in amounts quantified by numerical criteria unconnected to the substance of the investigation. This set of practices, while subtle, can change essential dimensions of public legal processes in the absence of sufficient inquiry into whether the changes are desirable. Thus, in Section IV.B, I question our collective indifference to how companies respond to third-party searches for internet evidence.

In Section IV.C, I suggest that judicial oversight, in its current form, will likely not suffice to provide the understanding and oversight of company practices necessary to control companies' tendency to displace case-specific application of legal norms with internal organizational protocols as the determinant of search scope. Accordingly, I contend in Section IV.D that a variety of institutional interventions should be considered to supplement existing judicial oversight.

A. Untethering Search Procedure

Under the Fourth Amendment to the U.S. Constitution, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[217] Probable cause exists when a "fair probability" exists that a search will result in evidence of a crime being discovered.[218] The particularity requirement is met when a warrant "enables the searcher reasonably to ascertain and identify the things to be seized."[219] Particularity is the requirement that a warrant clearly state the items being sought and where those items are thought to be located.[220] It is a function

[217] U.S. Const. amend. IV.

[218] Illinois v. Gates, 462 U.S. 213, 238 (1983).

[219] United States v. Santarelli, 778 F.2d 609, 614 (11th Cir. 1985); see also Marron v. United States, 275 U.S. 192, 196 (1927) (describing the particularity requirement as necessitating that "nothing is left to the discretion of the officer executing the warrant"); United States v. George, 975 F.2d 72, 75 (2d Cir. 1992).

[220] *Marron*, 275 U.S. at 196.

of the substantive context of an investigation, including the circumstances giving rise to probable cause for the search.[221]

The Fourth Amendment does not necessarily require a search warrant for most demands for internet data.[222] The Supreme Court has developed the "third-party doctrine," which provides that the Fourth Amendment does not apply to information revealed to third parties, particularly if it was revealed voluntarily.[223] Various statutes and judicial opinions, however, limit the scope of the third-party doctrine by imposing a warrant requirement for government bodies to obtain certain forms of data.[224] Further, in *Carpenter v. United States*, the Supreme Court refused to apply the third-party doctrine to historical cell-phone location data, over a certain time period, that is held by third parties.[225] Growing statutory and constitutional obligations for warrants suggest that for many forms of third-party internet evidence, a warrant comporting with Fourth Amendment principles and procedures will be required.

For judges to issue such warrants, they must review a warrant application to assess probable cause and particularity. This assessment requires an analysis of the sufficiency of the connection between the suspected criminal activity, the things to be seized, and the place to be searched.[226] To undertake this task, judges read the affidavit submitted by the police, and sometimes, they email or speak with the requesting officer by phone or in person to obtain the case knowledge needed to consider

[221] *Santarelli*, 778 F.2d at 614; *George*, 975 F.2d at 75–76; United States v. In re Search of Info. Associated with Fifteen Email Addresses, No. 17-cm-03152, 2017 WL 4322826, at *5 (M.D. Ala. Sept. 28, 2017).

[222] United States v. Miller, 425 U.S. 435, 443–44 (1976); Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[223] See Bellovin et al., supra note 46, at 25 ("The third-party doctrine, taken in its strongest expression in *United States v. Miller*, suggests that, once data is disclosed to a third party, it no longer receives Fourth Amendment protection . . . .").

[224] For example, the federal Stored Communications Act addresses the lack of Fourth Amendment protection for these data by "creat[ing] a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." Kerr, supra note 21, at 1212. CalECPA also requires all government agencies, including police and prosecutors, to obtain a search warrant to access almost all internet evidence. Cal. Penal Code § 1546.1(a)(3), (b)(1) (West 2017). When courts issue warrants under CalECPA, they are required to follow standard procedures for warrant application, such as warrants being issued upon a finding of probable cause, supported by an affidavit. Freiwald, supra note 64, at 153.

[225] 138 S. Ct. 2206, 2221 (2018).

[226] 2 Wayne R. LaFave, Jerold H. Israel, Nancy J. King & Orin S. Kerr, Criminal Procedure § 3.3(g), at 165–66 (4th ed. 2015).

the type of crime at issue, the extent of a suspect's ability to conceal evidence, the nature of the evidence sought, and the reasonable inferences that can be drawn from the affidavit.[227] Judges also have experience presiding over criminal cases, which means that they tend to have familiarity with the requirements of criminal law and types of evidence used to establish elements of particular crimes and, thus, which types of evidence agents are authorized to seek.

When companies execute search warrants, they appear to engage in an analogous assessment. However, that assessment relies on organizational criteria rather than on legal and substantive facts to determine the scope of evidence to be produced, as consistent with the Fourth Amendment. Organizational criteria are criteria—independent of a case's specific facts or circumstances—used by company staff to determine the types and amount of data to be produced in response to compulsory legal process. Company reviewers apply organizational criteria because they have little or no information about the substance of the case from which to assess what evidence would or would not be material and the quantity of data called for by warrant language may be great. As discussed earlier, companies typically do not receive the affidavit, and their staff often lack knowledge of what elements must be established to prove the associated crimes in court or what defenses might be available.[228]

In place of knowledge about particular cases and domain knowledge in criminal law, company staff turn to their internal knowledge about the company's products. When they review warrants, they tend to elevate organizational criteria such as dates, numbers of accounts, data size, and concerns about the ease and difficulty with which the data can be produced as the benchmarks of what should or should not be produced, without reference to the substantive particulars of the investigation or the elements of the offenses at issue.

On the surface, companies' application of organizational criteria resembles judicial review of search warrants for internet and digital evidence, which may also rely on criteria such as time limits, the types of communications involved, and the number of accounts affected.[229]

[227] Van Duizend et al., supra note 51, at 51 ("[M]ost [judges] told us they read through the application, trying to identify the links between what was presented in the affidavit and what was sought in the warrant.").

[228] See supra Section III.A.

[229] See, e.g., United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017) (discussing concerns with warrant seeking "virtually every kind of data that could be found in a social media

However, the way courts narrow the scope of the evidentiary demands in warrants based on these factors differs from how companies narrow the scope of their data production based on these criteria because judges consider the relationship between the specific warrant language, the circumstances supporting probable cause, and the crimes charged, as required under the Fourth Amendment.

Consider the example of search warrants seeking "all data." Judges are also concerned with such language—finding that it fails to "describe with particularity what will be searched" and to "establish a sufficient nexus between the place to be searched and the probable cause that would allow it."[230] In some cases, however, judges permit searches of "all records" when probable cause permits such a search, for example, when the affidavit presents evidence that a personal email account was used extensively in committing a crime.[231] Likewise, when courts limit the dates for which data will be produced, they focus on case circumstances—comparing the dates and times of events noted in the affidavit with the dates and times for which data are sought in the warrant.[232] When company staff narrow the scope of data production based on time, however, they usually do so not by reference to the particulars of cases but by reference to more arbitrary ranges of time periods, such as one week,[233] based partly on how long it would take to produce data covering more extensive periods of time.

This untethering has implications for the truth-seeking aims of adversarial systems, though the consequences of these practices are difficult to measure. This is because the impact of evidence—its meaning,

account"); Wheeler v. State, 135 A.3d 282, 304 (Del. 2016) (noting "Federal Courts of Appeals have concluded that warrants lacking temporal constraints, where relevant dates are available to the police, are insufficiently particular" and citing multiple cases); People v. Thompson, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019) (focusing on time constraints); United States v. In re Search of Info. Associated with Fifteen Email Addresses, No. 17-cm-03152, 2017 WL 4322826, at *5–8 (M.D. Ala. Sept. 28, 2017); cf. Van Duizend et al., supra note 51, at 51 (describing how judges reviewing warrants to search physical properties used mental checklists that included "time, place, leads, reliability, jurisdiction, substantiation, specificity, adequate address or description").

[230] *Fifteen Email Addresses*, 2017 WL 4322826, at *7.

[231] United States v. Bowen, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) ("The fact that Defendants chose to use the same e-mail accounts for personal communications that they were simultaneously using to conduct their allegedly fraudulent business cannot insulate those e-mail accounts from a search pursuant to the all records exception.").

[232] United States v. Bickle, No. 10-cr-00565, 2011 WL 3798225, at *21 (D. Nev. July 21, 2011).

[233] See supra text accompanying notes 166–69.

weight, and importance—are context and case specific and often cannot be known until various pieces of evidence are gathered and compared. For instance, evidence may include materials establishing a person's identity, the nature of a relationship between individuals, or an individual's mental state at a particular time.[234] What constitutes evidence also depends on the kinds of exculpatory explanations that suspects have offered.[235] In addition to establishing alibis, digital evidence can help establish affirmative defenses, impeach and undermine the credibility of victims and witnesses, and show that certain elements of crimes have not been proven.[236] By deciding which data to produce among the various types of data that may be responsive, companies shape the legal and factual theories that both prosecutors and criminal defendants can ultimately advance in court.

Consider this example based on a case recounted by one prosecutor.[237] In this case, he knew a suspect had used a particular email account—let us call it business@email.com—to facilitate illegal sales. He needed to establish that the suspect was indeed the person who had used that account during a specific period, and thus he required evidence not only from business@email.com but also from the suspect's personal email address—let us call it personal@email.com—where the suspect discussed events in his personal life that matched up with events that he had also mentioned in the account used for illegal sales. For example, the suspect may have discussed fixing his car on particular dates in emails from business@email.com while also mentioning getting his car fixed in emails to his brother sent from personal@email.com.

An investigator wanting to firmly establish the identity of the person using the business account might reasonably want two years of data from the personal account to establish several such examples. Nevertheless, a company reviewer not privy to the warrant affidavit would likely not understand how years of emails from the personal account would be relevant and would try to narrow the period for which data is produced. An investigator, who does not necessarily know how valuable two years

[234] See generally Bambauer, supra note 4 (discussing the police interests in third-party searches).

[235] Fairfield & Luna, supra note 4, at 986 ("With citizens' lives increasingly logged and tracked, online and off, the chance of finding evidence tending to prove innocence only increases.").

[236] See Wexler, supra note 4, at 2723; Fairfield & Luna, supra note 4, at 984–86, 1030–31; Brandon L. Garrett, Big Data and Due Process, 99 Cornell L. Rev. Online 207, 207 (2014).

[237] Interview with Prosecutor 5 (Nov. 2021) (transcript on file with author).

of data will be, may very well decide that data covering a shorter period are sufficient.

In such a case, it is possible that whatever evidence produced by the company is sufficient for the prosecutor to establish the identity of the account owner, or the identity evidence may be strong enough to file a case but insufficient to prevail at preliminary proceedings. Alternatively, the reduced amount of data may mean that the prosecutor fails to see evidence suggesting that another person—in addition to the suspect—used the account.

The consequences for defendants are equally difficult to ascertain.[238] Much of a defendant's or defense counsel's evidence is initially acquired by prosecutors or police officers through discovery. An officer's receiving one less year of data effectively means that the criminal defendant will likely also have one less year of data to establish a defense—in the above example, he might be deprived of evidence that another person used his business email account. Because law enforcement access to evidence is often the only way that defendants obtain access to evidence,[239] the failure of a law enforcement agent to obtain data may mean that evidence is also denied to the defendant.[240]

Untethering also contributes to a cycle of mutually reinforcing company opacity and broad search warrant language. Judges and commentators have criticized law enforcement for drafting broad search warrants that seek too much data for too many accounts. Indeed, judges themselves have been criticized for deferring too much to agents,[241] "rubber stamp[ing]" warrant applications without sufficient review of

[238] Cf. Wexler, supra note 4, at 2727 (arguing that the "full scale of harm to the truth-seeking process" of the "consensus view" on criminal defense subpoenas under the SCA is "difficult to grasp").

[239] Erin Murphy, The Mismatch Between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System, 87 S. Cal. L. Rev. 633, 639 (2014) ("Typically, a defendant has virtually no right to have particular evidence collected and preserved. Instead, these tasks fall largely within the purview of the government as a corollary to its burden of proof and persuasion.").

[240] Id. at 641 (discussing how evidence may be erased before it can be accessed by defense counsel, "who often must wait until formal charging or the setting of a trial date to leverage the subpoena power and who also lack the coercive authority of police").

[241] See, e.g., Anna Lvovsky, The Judicial Presumption of Police Expertise, 130 Harv. L. Rev. 1995, 1998–99 (2017); Osagie K. Obasogie & Zachary Newman, The Endogenous Fourth Amendment: An Empirical Assessment of How Police Understandings of Excessive Force Became Constitutional Law, 104 Cornell L. Rev. 1281, 1287 (2019).

either probable cause or particularity,[242] and "fail[ing] to supply meaningful limits . . . in reviewing searches after the fact at a suppression hearing."[243] However, even when judges have denied warrants on the grounds of insufficient particularity, law enforcement agents are sometimes unwilling to craft narrower search demands.[244]

My findings suggest that the problem of broad warrants is not just a matter of excessive zeal on the part of government agents or undue judicial deference. Rather, this excessive breadth may also stem from the cyclical interplay of officers' efforts to draft warrants using the language most likely to get them the evidence that they have probable cause to seek and the often opaque, inconsistent, and arbitrary ways in which companies respond to the warrant language composed by agents poorly informed of the nature and structure of company data holdings. As discussed in Section II.D, companies' practices often lead evidence seekers to perceive company decisions as arbitrary—particularly when staff within one company interpret the same language appearing in different warrants differently.[245]

The opacity of company practices further exacerbates law enforcement's perception that companies are inconsistent and arbitrary. The interview data suggest that companies try to insulate staff and information about company policies and practices and that, thus, reviewers often make production decisions privately. They often do not disclose to anyone outside the company that they have decided to produce—or not produce—certain data, or the reasons behind their decisions.[246] When companies do occasionally communicate their decisions, they do not necessarily give a complete account of what data were withheld and why.[247] Thus, even if companies are internally

[242] See Oren Bar-Gill & Barry Friedman, Taking Warrants Seriously, 106 Nw. U. L. Rev. 1609, 1639 (2012) (reviewing literature criticizing judges for rubber-stamping warrants).

[243] Laurent Sacharoff, The Fourth Amendment Inventory as a Check on Digital Searches, 105 Iowa L. Rev. 1643, 1651 (2020).

[244] In re Search of Info. Associated with [redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 2 (D.D.C.), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014) ("Despite this Court's repeated prior warnings about the use of formulaic language and overbroad requests that—if granted—would violate the Fourth Amendment, this Court is once again asked by the government to issue a facially overbroad search and seizure warrant. For the reasons explained below, the government's application for a search and seizure warrant will be denied.").

[245] See supra text accompanying notes 113–16.

[246] Interview with Outside Counsel 4, supra note 94.

[247] See id.

applying consistent—and justifiable—policies, they may still appear arbitrary because those policies are not externally known.

To shield against companies' apparent inconsistency and arbitrariness, law enforcement errs by drafting broad and inclusive warrants—in fear that using more precise or narrower language may lead to the production of even less data by companies. In other words, agents may feel obligated to list more categories of data to address concerns that companies will withhold responsive data based on company reviewers' particular readings of terms in search warrants. By including more categories of data, however, law enforcement further subjects companies to knowledge misalignment, which companies manage, again, with a set of makeshift practices that may lead them to inconsistently produce data.[248]

This set of dynamics means that the search conducted in response to a search warrant, and thus the evidence that is ultimately produced, may become less and less a matter of what the judicially endorsed language calls for in a warrant. As discussed earlier, the processes that companies have developed to respond to search warrants do not, for the most part, reflect deliberate company efforts to facilitate or frustrate government efforts to access evidence, nor do they suggest deliberate company efforts to displace the authority of judicial officers as the authoritative decision-makers concerning the scope of search warrants. Company practices are, rather, a series of makeshift expedients for coping with genuine predicaments arising from imprecise or impracticable wording in warrants.

All the same, these company practices are worrisome because, under Fourth Amendment procedures, the scope of a search is supposed to be visible from the face of the warrant. The particularity requirement is met only when a warrant is written with sufficient granularity such that the executing officer can identify those items that the magistrate has authorized to be seized with reasonable certainty.[249] When companies

[248] This set of conditions is likely exacerbated by the fact that, at the local level, police investigators in small- and medium-sized agencies may work for a few years in an investigative role before being rotated out of their position. A new detective, interacting anew with the company, may again use imprecise and "wrong" language. See supra text accompanying notes 149–51.

[249] United States v. Santarelli, 778 F.2d 609, 614 (11th Cir. 1985); United States v. George, 975 F.2d 72, 75 (2d Cir. 1992); United States v. In re Search of Info. Associated with Fifteen Email Addresses, No. 17-cm-03152, 2017 WL 4322826, at *5 (M.D. Ala. Sept. 28, 2017);see Nicole Friess, When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance, 90 Neb. L. Rev. 971, 986 (2012).

reconstruct warrants without sufficient notice to others, one of the core aims of search warrants—explicit delimiting of searches—is undermined.

Thus, although company practices are sufficiently responsive that officers have, in the main, acquiesced in them, these practices nevertheless entail determining the scope of searches through criteria that often enough call for both more and less data than would be produced under an assiduous effort to carry out the search as described in the warrant's language. In this way, the operation of knowledge misalignment—and the efforts of company staff to cope with it across thousands of cases—is necessary to understand the origins of the subtle institutional changes that untether the scope of third-party evidence production from the legal principles and search warrant language that are supposed to govern the process.

B. Challenging Our Acquiescence

As the above analysis suggests, the untethering of search procedure is not a dramatic process: many companies neither wholeheartedly embrace nor resist their role as evidentiary intermediaries. However, their emergence as evidence intermediaries whose staff now carry out a core legal activity—executing search warrants—previously performed by public officials has shifted the organizational locus and dynamics under which that activity is carried out. As scholars of organizations recognize, significant change can unfold through relatively gradual processes.[250] Here, substantial changes in search procedure can occur through acquiescence in convenient routines and steady renewal of habits,[251] leading to the gradual erosion of formal legal principles through disuse. Here, in addition, the untethering of search procedure exemplifies the

[250] E.g., Martha S. Feldman & Brian T. Pentland, Reconceptualizing Organizational Routines as a Source of Flexibility and Change, 48 Admin. Sci. Q. 94, 115 (2003); Martha S. Feldman & Anat Rafaeli, Organizational Routines as Sources of Connections and Understandings, 39 J. Mgmt. Stud. 309, 310 (2002); Martha S. Feldman, Organizational Routines as a Source of Continuous Change, 11 Org. Sci. 611, 626–27 (2000); Martha S. Feldman, Brian T. Pentland, Luciana D'Adderio & Nathalie Lazaric, Beyond Routines as Things: Introduction to the Special Issue on Routine Dynamics, 27 Org. Sci. 505, 508 (2016); Brian T. Pentland & Henry H. Rueter, Organizational Routines as Grammars of Action, 39 Admin. Sci. Q. 484, 484 (1994).

[251] Moshe Farjoun, Christopher Ansell & Arjen Boin, Pragmatism in Organization Studies: Meeting the Challenges of a Dynamic and Complex World, 26 Org. Sci. 1787, 1797 (2015) (discussing how routines and habits lead to organizational and institutional change).

subtle ways in which legal institutions change and adapt in the information age.[252]

Of course, it is neither unexpected nor necessarily bad that legal procedures undergo changes as they operate in the context of the information economy. As Julie Cohen has pointed out, "the movement to informational capitalism puts new resources, new economic logics, and new technological affordances into play."[253] We should not assume that the capacity of institutions such as compulsory legal process and adversarial litigation to achieve the aims entrusted to them will remain unchanged by major society-wide developments, nor should we view the process that blackletter search law prescribes and the roles that it assigns to police, prosecutors, judges, and other actors as the ideal state of affairs. My position is not that the pre-internet compulsory process represents a better state of affairs.

Instead, I identify these organizational dynamics to question our relative indifference to internet technology companies' actual data production practices in response to compulsory legal process. Recent literature concerning evidence intermediaries focuses on the potential salutary effects of company decisions on user privacy—especially the privacy of users unconnected with an investigation whose data may be obtained by state agents.[254] The underlying intuition is that, when companies narrow the scope of information provided to law enforcement, companies are safeguarding users' privacy against government intrusion.[255] Indeed, during the research interviews, I found substantial evidence for this pro-privacy account. For example, company efforts to limit the scope of government searches of their data to what company staff deem appropriate while also meeting what company staff guesses are the requesting officers' genuine investigative needs may very well result in searches that are both less intrusive of customer privacy and more fruitful in delivering relevant evidence.

Nonetheless, my findings also caution against embracing this view of companies' evidentiary role. First, the interview data suggest that the beneficial consequence of additional privacy protection is largely incidental to the series of makeshift practices unilaterally undertaken by

[252] Cohen, supra note 12, at 2 ("We are witnessing the emergence of legal institutions adapted to the information age, but their form and their substance remain undetermined.").

[253] Id. at 143.

[254] See supra notes 16–17 and accompanying text.

[255] E.g., Rozenshtein, supra note 5, at 124–25, 133–34.

companies managing the informational and communication challenges of increasing third-party process demands.[256] Second, even if companies appear to be making the "right" calls, few mechanisms exist to determine the "right" call or whether companies are the right actors to make those calls.[257] As a society, we should be wary of also acquiescing in companies' decisions about a public procedure so closely and importantly controlled by law—particularly when those practices appear to untether search procedure from the factual and legal analysis consistent with the Fourth Amendment.

We should also be worried about a set of processes that lets formal legal actors, such as law enforcement and judicial officers responsible for overseeing the process, readily acquiesce to company practices. Institutionally, companies' practices enable evidence requesters—and reviewing judges—to abdicate their responsibility to learn how to prepare—and review—warrants that are meaningfully particular concerning the data holdings of specific companies. A search warrant is, after all, a *judicial* order to *an officer* to carry out the search. The officer who has sought the warrant and the court who has approved it both have the responsibility to understand whether companies have responded with sufficient fidelity to the judicial directive. If the officer and the authorizing court fail to inquire why specific data were produced or not produced, they fail to carry out some of their duties, including ensuring that the search was executed faithfully to the terms of the judicial order.

C. The Limits of Judicial Capacity

My study also raises substantial questions about the existing capacity of judicial officers to oversee problematic company practices. In this Section, I argue that judicial officers are currently ill-equipped to oversee the kinds of company practices revealed by the interview data and that various institutional interventions to supplement existing court oversight of search procedure should be considered.

The primary reason that judicial officers are currently ill-suited to oversee contemporary third-party search procedure for internet evidence

[256] See supra Sections II.D & III.B.

[257] See Cover, supra note 8, at 1473, 1478–79, 1485; Paul Ohm, The Microsoft Design Decisions That Caused This Mess, Just Sec. (Feb. 21, 2018), https://www.justsecurity.org/52805/microsoft-design-decisions-caused-mess/ [https://perma.cc/JAY4-WWEC]; Kiel Brennan-Marquez, Beware of Giant Tech Companies Bearing Jurisprudential Gifts, 134 Harv. L. Rev. F. 434, 434 (2021).

is that judges face knowledge misalignment regarding company data holdings that is similar to—and likely more significant than—that faced by law enforcement agents. In the instant context, judges cannot fully overcome the types of knowledge problems encountered by law enforcement, mainly, the vast and varying scope of company data practices. After all, the problems at issue concern not simply knowledge about a single company but new and different bodies of knowledge for many companies. For judges, as for law enforcement, developing sufficient knowledge requires understanding company-specific data holdings and operations, which can vary across companies and across time. Thus, even if judges successfully learn enough about some company practices to narrow searches, their knowledge will often become outdated or irrelevant as companies develop their products or reconfigure their technical architecture. As Orin Kerr has argued, judges operate with an "[i]nformation [d]eficit" and limited time and expertise to gather the information necessary to understand specific technologies or how those technologies fit into the broader information and social environment.[258]

Judicial oversight is also limited because it depends on adversarialism on the part of prosecutors and criminal defense attorneys. In criminal proceedings, litigation with evidence-holding third-party companies is infrequent because it is generally incidental to the central conflict of the case before a judge: that between the prosecution and the criminal defendant. This positionality likely reduces the resources that prosecutors and defense counsel are willing to devote to a collateral dispute with a company over evidence production, making sustained efforts to investigate and challenge a company's practices in court all the less frequent. Thus, many issues concerning company practices are not litigated, even if they are known.

Furthermore, although criminal litigation is adversarial in that there are two opposing parties—prosecution and defendant—in any given case, at

[258] Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 807, 875–76 (2004) [hereinafter Kerr, The Fourth Amendment and New Technologies]; Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241, 1283 (2010) [hereinafter Kerr, Ex Ante Regulation] ("The judge can modify the warrant, but his primary decision is whether to sign or reject it. The entire process takes a matter of minutes from start to finish. No hearing occurs. There is no testimony beyond the affidavit in most cases, and the affidavit usually contains only standard language about computer searches. A prosecutor may be present, but need not be. Obviously, no representative of the suspect is present to offer witnesses or argument."); Van Duizend et al., supra note 51, at 26, 49.

least one of those parties' positions is usually not adversarial with respect to a third party's willingness or reluctance to produce or withhold evidence. For any given motion to compel, quash, or suppress, whether the prosecution or defense favors or opposes a third-party company's decisions concerning the data at issue depends on the anticipated valence of those data as evidence in the case. Accordingly, whatever decision the company had made—either to produce or withhold data, or to change what data is produced—will generally receive the further support of one of the two parties to the case.[259] This means that, even if the overall institutional interests of both prosecuting agencies and defense attorneys favor greater transparency, this commonality of interest does not translate to sustained litigation pressure on companies to produce evidence consistently or transparently. In turn, when parties do not adequately litigate company practices, judges have little opportunity to exert oversight of the process.

Even when matters are litigated, judges sometimes make poorly informed assumptions about what happens when officers execute a search warrant for company-held data. As Kerr reminds us, in *United States v. Bach*, an earlier case involving "a constitutional challenge to the law enforcement practice of faxing search warrants to" companies, the district court overlooked differences in the processes and privacy implications of searching physical property versus searching computer servers.[260] On appeal, Yahoo! and a group of other companies filed an amicus brief explaining that searches for information stored on internet service providers' servers require technical expertise and specialized knowledge to extract the relevant data from company networks.[261] The U.S. Court of Appeals for the Eighth Circuit subsequently concluded that faxing warrants was constitutionally reasonable.[262]

More recently, judges have continued to misunderstand company processing—with some assuming that obtaining internet evidence from companies is a simple matter where companies readily produce the

[259] One atypical example is San Diego County District Attorney Intervenor Brief at 11–16, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203) (arguing that the SCA should not block criminal defense subpoenas to Facebook).

[260] Kerr, The Fourth Amendment and New Technologies, supra note 258, at 877–79. (discussing United States v. Bach, No. 01-cr-00221, 2001 WL 1690055, at *1–3 (D. Minn. Dec. 14, 2001), *rev'd*, 310 F.3d 1063 (8th Cir. 2002)).

[261] Id. at 879 (discussing Brief of Amici Curiae Yahoo!, Inc., et al., In Support of Appellant United States of America and Urging Reversal at 6–7, *Bach*, 310 F.3d 1063 (No. 02-01238)).

[262] *Bach*, 310 F.3d at 1065.

categories of data enumerated in a search warrant.[263] Consider this appellate opinion in which the judge appears to assume that Facebook will reliably produce the data sought by officials:

> Hard drive searches require time-consuming electronic forensic investigation with special equipment, and conducting that kind of search in the defendant's home would be impractical, if not impossible. By contrast, when it comes to Facebook account searches, *the government need only send a request with the specific data sought and Facebook will respond with precisely that data*.[264]

As this Article has shown, responding to a request that identifies the specific data that an officer seeks is often not a clear-cut matter, and "precisely" responding with data can be quite far from company practice in fact.[265]

This is not to say that judicial officers can never exert effective oversight. Many judicial officers have substantial experience with search warrants—and with related issues in civil discovery—and some are fairly well informed about electronic evidence.[266] The Foreign Intelligence Surveillance Court—a small court of federal district court judges appointed to review surveillance applications under the Foreign Intelligence Surveillance Act of 1978 ("FISA")—has developed substantial expertise in the types of information and data sought by national intelligence agencies.[267]

On the whole, however, generalist judicial officers lack the resources and time to develop this type of expertise. The FISA Court, for example, has staff attorneys who do initial reviews of applications and identify

[263] E.g., United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017); In re Search of Info. Associated with [Redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 153 (D.D.C.), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014) ("[T]he electronic communication service provider . . . can perform the search at the government's request and turn over any relevant data that it discovers.").

[264] *Blake*, 868 F.3d at 974 (emphasis added).

[265] See supra Part III.

[266] See Emily Berman, Digital Searches, the Fourth Amendment, and the Magistrates' Revolt, 68 Emory L.J. 49, 61–65 (2018) (describing judges who have written substantially on search warrants for electronic evidence); Seth Katsuya Endo, Discovery Hydraulics, 52 UC Davis L. Rev. 1317, 1338–41 (2019) (describing judges and judicial efforts to study and reform civil discovery of electronic evidence).

[267] Margo Schlanger, Intelligence Legalism and the National Security Agency's Civil Liberties Gap, 6 Harv. Nat'l Sec. J. 112, 136, 163–66 (2015) (describing judicial opinions scrutinizing National Security Agency demands for data and characterizing FISA judges as having "intense judicial involvement" in minimizing data sought by the agency).

additional questions to ask of law enforcement.[268] The FISA context is also one in which companies may be willing to be more open about their data practices and holdings, in part because the recipients of the information—intelligence officers and judges with security clearances—are under independent obligations not to reveal information about companies.[269] Likewise, in discovery disputes, the parties are often able to bring to the judge's attention problematic production practices of the other party, in part because the parties have more information about the types of evidence that likely exist, and they are more confident that the other party has an interest in not making that information available.[270] These dynamics, resources, and legal procedures that may lead to more adversarialism in civil discovery are absent in the third-party search context.

That being the case, proposals that seek to rely on existing oversight mechanisms are unlikely to be adequate. In recent years, scholars and legislators have proposed the idea of requiring a detailed inventory[271] of searches for digital evidence on devices and from internet service providers. For example, under Laurent Sacharoff's proposal, "[l]aw enforcement should be required to make an accounting of the files, emails, or other information they obtain . . . [and] look at" and to distribute a copy of the return to the subject of the search, whether a "suspect, defendant,

[268] Letter from Hon. Reggie B. Walton, Presiding J., U.S. Foreign Intel. Surveillance Ct., to Hon. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary 2, 5–6 (July 29, 2013), https://irp.fas.org/news/2013/07/fisc-leahy.pdf [https://perma.cc/PC5Y-6T8A].

[269] See Berman, supra note 266, at 72–77, 80, 85 (discussing, inter alia, the multipronged approach the FISA Court has implemented to protect data privacy).

[270] David Freeman Engstrom & Jonah B. Gelbach, Legal Tech, Civil Procedure, and the Future of Adversarialism, 169 U. Pa. L. Rev. 1001, 1047 (2021). See generally Neel Guha, Peter Henderson & Diego A. Zambrano, Gamesmanship in Modern Discovery Tech, *in* Legal Tech and the Future of Civil Justice 112 (David Freeman Engstrom ed., 2023) (discussing various aspects of high-tech discovery tools that provide opportunities for data manipulation by parties).

[271] Federal Rule of Criminal Procedure 41 requires officers to create an inventory of every item seized during a search and provide that list to the magistrate judge, who must provide it to the suspect, if requested. Fed. R. Crim. P. 41(f)(1)(B), (D). Many state statutes require that officers do the same, usually within ten days of the warrant's issuance. Van Duizend et al., supra note 51, at 36. This "return" specifies whether the warrant was executed, the date and time of service, and what was seized. Id. The inventory is commonly filed after searches of physical spaces, but judges have not imposed the requirement meaningfully for searches of electronic evidence. See Sacharoff, supra note 243, at 1663 (discussing searches of electronic devices). Indeed, for searches of electronic devices, Rule 41 does not require officers to list the files opened and viewed. Fed. R. Crim. P. 41(f)(1)(B).

or witness."[272] Recent federal bills have also contemplated modifying Rule 41(f)(1)(B) of the Federal Rules of Criminal Procedure to require the filing of an inventory that "disclose[s] whether the provider disclosed to the government any electronic data not authorized by the court and, if so, provide[s] detailed information regarding the disclosure."[273] Given the difficulties faced by investigators in identifying the various types of data held and produced by companies, and the challenges that company staff face in discerning precisely what is called for by imprecise or highly broad warrant language, it is unrealistic to think that the same officers will be capable of precisely enumerating the data that they received or of meaningfully comparing it to what was called for by their search warrant.

In theory, inventories could help judges develop a more robust understanding of the kinds of data that companies hold, and can produce, because a detailed inventory would allow the judge to compare the data sought in a warrant with the actual categories of data produced. This knowledge would facilitate better review of the execution of the search for reasonableness ex post by enabling the judge to have, at a motion to suppress, a better general sense of the kinds of data that companies typically have and produce in response to particular search warrant language, against which to compare the circumstances of the search in the specific case before them.[274] At the ex ante stage, when judges review warrant applications, knowledge from reviewing past search inventories could supply a better sense of how types of data should be enumerated in a search warrant to avoid language that is unclear or too broad in scope.

In fact, however, an inventory is likely insufficient to build the capacity of judges to understand internet technology companies' data practices, including when reviewing warrants, querying data sets, and producing evidence. First, the potential benefits discussed above depend on internet technology companies being willing to provide officers with detailed information about their data holdings so that officers can compose inventories that intelligibly enumerate the categories of data sought and produced under a search warrant. Second, the success of the inventory also depends on adversarialism on the part of prosecutors and criminal

[272] Sacharoff, supra note 243, at 1665–66; id. at 1665 ("I have limited my proposal to devices, but many of my arguments apply with some adaption to third-party subpoenas or warrants from electronic providers.").

[273] Government Surveillance Transparency Act of 2022, S. 3888, 117th Cong. § 3(c) (2022).

[274] See Kerr, Ex Ante Regulation, supra note 258, at 1280 (discussing how case law on reasonableness is developed during ex post review).

defense attorneys, which tends to be infrequent, as discussed above, because it is incidental to the central conflict of criminal cases.[275] On the whole, then, there are strong reasons to question the sufficiency of judicial oversight as the sole institutional mechanism for overseeing search warrant procedure.

D. Toward Institutional Interventions

In this Section, I argue that a variety of institutional interventions should be considered to supplement judicial oversight of third-party search procedures in which internet technology companies play a substantial role. One such set of measures may involve the adaptation of civil discovery procedures within criminal procedure. While the positionality and incentives of internet technology companies as evidence intermediaries differ from those of parties obligated to produce evidence during discovery,[276] litigants also encounter information and communication problems in the course of seeking evidence from complex organizations. The Federal Rules of Civil Procedure incorporate several mechanisms to address such problems in litigation, including interrogatories, privilege logs, requirements for parties to meet and confer, and special masters.[277] Adapting some of these mechanisms in criminal procedure may be necessary to address the substantial role that internet technology companies—with broad and frequently changing data holdings—play in third-party search procedure.

A second way to strengthen the oversight capacity of judges may be to expand the ambit of the administrative bodies of courts—such as the Administrative Office of the U.S. Courts ("AO") or state equivalents—to include conducting systematic reviews of search warrants and

[275] Where search warrants have been litigated, however, litigation has produced useful information about company practices, such as in the context of geofence search warrants or companies' storage of data stored overseas. E.g., In re Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 712–13 (E.D. Pa.), *aff'd*, 275 F. Supp. 3d 605 (E.D. Pa. 2017); In re Google, LLC, 542 F. Supp. 3d 1153, 1156 (D. Kan. 2021); In re Search of Info. That Is Stored at the Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 70–71 (D.D.C. 2021); United States v. Chatrie, 590 F. Supp. 3d 901, 907–16, 926, 936 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024); Order Granting Motion to Quash Geofence Search Warrant at 6–13, 35–36, People v. Dawes, No. 19002022 (Cal. Super. Ct. Sept. 30, 2022), https://www.eff.org/document/people-v-dawes-order-granting-motion-quash-geofence-warrant-california [https://perma.cc/C9T5-GGSZ] (order granting motion to quash geofence search warrant).

[276] See supra Section I.A.

[277] Fed. R. Civ. P. 26, 33, 34, 53.

corresponding data produced by companies. The AO may be a reasonable institution to develop and undertake this function. As the home of the Wiretap Reports[278] and Delayed-Notice Search Warrant Reports,[279] it is already responsible for gathering and publishing information about company- and technology-mediated evidence gathering by law enforcement. Institutionalizing the systematic review of search warrants and company productions within courts' administrative offices may help generate critical "systemic facts" for the judicial officers and courts to understand company and law enforcement search procedures.[280]

The review of third-party search production may also help evaluate the necessity of a third potential intervention: the creation of a national information-coordination body funded by Congress. Jennifer Daskal and William Carter have proposed the creation of a new national office that would, among other things, generate and disseminate information about company practices among judges, investigators, prosecutors, and criminal defense counsel.[281] For example, the office would conduct research and develop a "centralized repository of knowledge and expertise" about companies' systems and "procedures for submitting requests for data."[282] In addition, the office could provide training and produce training materials for courts and various evidence-seeking legal parties.[283]

While the idea of a national office may seem drastic, my interview findings suggest that the information collection and exchange functions contemplated by Daskal and Carter's proposal are likely to be more effective in helping legal actors—investigators, prosecutors, defense counsel, and judges—develop the capacity necessary to understand company practices than would a more robust search warrant requirement alone. Both the research activities and the training contemplated by their national office proposal could help to sustain a repository of regularly updated and reasonably thorough information about what kinds of data

[278] See 18 U.S.C. § 2519(3); Wiretap Reports, U.S. Cts., https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports [https://perma.cc/N7QH-87DD] (last visited Apr. 8, 2024).

[279] See 18 U.S.C. § 3103a(d)(2); Delayed-Notice Search Warrant Report, U.S. Cts., https://www.uscourts.gov/statistics-reports/analysis-reports/delayed-notice-search-warrant-report [https://perma.cc/9CR7-9CYA] (last visited Apr. 8, 2024).

[280] Systemic facts are facts that facilitate institutional awareness of the behavioral patterns of legal system actors. Andrew Manuel Crespo, Systemic Facts: Toward Institutional Awareness in Criminal Courts, 129 Harv. L. Rev. 2049, 2052 (2016).

[281] Carter & Daskal, supra note 9, at 27–28.

[282] Id.

[283] See id. at 28.

are held by internet technology companies from whom legal parties frequently seek evidence, the nomenclature used at the companies to describe those data, and the companies' practices for producing such data.

The idea of a national office is also consistent with proposals from Freedom of Information Act ("FOIA") and evidence scholars advocating for institutions outside of individual judges to oversee information production by organizations. For example, FOIA requesters and agency responders often find themselves in situations similar to those faced by the law enforcement investigators and company staff studied here.[284] Scholars and practitioners alike have observed that the ways in which government agencies interpret FOIA requests can substantially affect the volume and quality of the information ultimately released.[285] This is especially evident when there is a "prerequisite knowledge problem," where requesters must possess sufficient knowledge about the government activities that they are requesting records about to obtain a meaningful response.[286]

Here, too, courts do not appear well equipped to oversee agencies' organizational practices for producing responsive information. Margaret Kwoka explains that courts are "reluctant to check agency secrecy," citing one study that found that agencies "prevailed in FOIA cases" at a greater rate than they succeeded in "other types of agency review, even though agencies are supposed to receive less deference in FOIA cases . . . ."[287] Perhaps even more critically, courts feel unduly burdened by the volume of FOIA cases.[288] Like search warrants, FOIA requests are high in volume and often drafted broadly.[289] Determining what data should and should

[284] Mark Fenster, The Opacity of Transparency, 91 Iowa L. Rev. 885, 907, 916–17, 942 (2006).

[285] See Margaret B. Kwoka, Delegating Information Oversight, Geo. L.J. (forthcoming 2024) (manuscript at 7, 10), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4382265 [https://perma.cc/ZV4E-99AA].

[286] David Alpert, Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech, 120 Colum. L. Rev. 1215, 1229 n.83 (2020) ("[V]eiled initiatives [including CIA torture and NSA surveillance programs cannot be successfully FOIA'd] until requesters discerned their existence. Indeed, mere hints and suspicions were inadequate; until identified with sufficient specificity that they could be the subject of reasonably precise inquiry, FOIA requests regarding such programs were likely . . . fruitless." (alterations in original) (quoting Seth F. Kreimer, The Freedom of Information Act and the Ecology of Transparency, 10 U. Pa. J. Const. L. 1011, 1025–27 (2008))).

[287] Kwoka, supra note 285, at 28.

[288] Id. at 30–31.

[289] Id. at 31.

not be produced in response to FOIA demands can require substantial work, increasing the volume of docket matters to be managed.[290]

In light of the courts' weaknesses in carefully reviewing FOIA disputes, Kwoka has argued for the creation of an independent information commission to review federal agencies' compliance with FOIA obligations.[291] She argues that a well-designed independent commission would be far superior to judicial review for reviewing FOIA disputes because it would increase the volume and availability of external review of agency decisions to withhold information.[292] Critically, a commission could also undertake different types of reviews, including inspections and audits.[293] As Kwoka points out, "[a]n information commission could develop the necessary expertise to critically examine these agency claims."[294]

In the closer domain of forensic evidence, Erin Murphy has argued for better regulatory oversight of evidence generated by "second-generation," or "2G," technologies, such as location tracking, facial recognition, and DNA.[295] Such 2G evidence "relies upon large-scale collections of data to obtain or provide meaning to evidence," is "developed fully or in part with the aid of private sector entities," and "requires complex and sophisticated knowledge and instrumentation to understand or interpret it."[296] Murphy argues that relying on individual lawyers and trials to identify problems with 2G evidence produced by private software vendors or public laboratories is inadequate because such an approach does not provide systematic safeguards of evidentiary integrity.[297] Instead, the adversarial system should aim for oversight that "focuses less on the happenings in a particular case and more on systemic and structural interventions."[298] In the context of forensic labs, for example, oversight entities could "undertake random unannounced inspections to ensure lab

[290] Id.
[291] Id. at 35.
[292] Id. at 37–40.
[293] Id. at 46.
[294] Id. at 41.
[295] Erin Murphy, The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence, 95 Calif. L. Rev. 721, 728, 777–88 (2007); Murphy, supra note 239, at 636–37, 658.
[296] Murphy, supra note 239, at 637 (emphasis omitted).
[297] Id. at 649–50, 652, 658.
[298] Id. at 659.

compliance with strict quality assurance standards,"[299] an idea reminiscent of the FOIA inspections suggested by Kwoka.[300]

Many of the concerns in the context of FOIA and 2G evidence are likely also to apply to judges reviewing third-party search production by companies. Judges are likely to feel burdened by the volume of search warrants for which they would be responsible for assessing the integrity of data production at a case-by-case level. Even if companies were entirely transparent regarding their data holdings and production practices, judges would likely find themselves without sufficient expertise to evaluate the fidelity and consistency of evidence production by companies.

Of course, the form of the commission that Kwoka has proposed, or of the inspection bodies suggested by Murphy, would likely differ from that of the particular institution needed in the context studied here. Nor is the national digital evidence office proposed by Daskal and Carter necessarily the proper organizational form. My aim in discussing these proposals is not to argue that these particular types of bodies should be *the* institutions to oversee the problems found in this study. Such an argument would require analysis and evaluation well beyond the scope of this Article.

Instead, I aim to link the knowledge misalignment theorized here to informational and communication problems in other legal contexts that depend on organizations to produce critical information. While FOIA, laboratory evidence, and internet evidence span different social and legal domains, they all depend on organizations to reliably produce information for public purposes. In addition, across these contexts, there is reason to believe that judicial oversight alone may be insufficient. This study suggests that internet data searches, as practiced, are becoming increasingly untethered from search law not merely in the occasional case but as a matter of course across thousands of compulsory data requests. When interorganizational interactions occur with the frequency of search warrants for internet data, various institutional interventions to supplement judicial oversight may very well be necessary.

The need for such interventions will likely grow as increasing numbers of companies become evidence intermediaries for information about the everyday activities of millions of people. Motor vehicles, for example,

[299] Id. at 659–60.
[300] Kwoka, supra note 285, at 46–47.

now carry integrated computers for diagnostics, navigation, and infotainment systems, all connected to online repositories of other information about people's movements, communications, and other activities.[301] Likewise, various smart home devices incorporate habit monitoring features, adding yet dozens of other activities for which companies now hold records that could potentially be sought and used as evidence.[302] The collection and exploitation of data is also becoming a central goal of organizations with long-established roles as evidence intermediaries, such as hospitals and banks.[303] As various organizations collect and store more information about individuals that is frequently sought for use in legal proceedings, those organizations' role in evidence production also becomes more extensive and complex. The current lack of institutions and mechanisms to systematically understand and oversee these developments will likely lead to even more acute versions of the problems identified in this Article.

CONCLUSION

Our Supreme Court has recently repeated the maxim that "[i]n our judicial system, 'the public has a right to every [person]'s evidence.'"[304] This commitment, backed by search warrants, subpoenas, and other forms of compulsory legal process, does not come without significant obligations falling on people and organizations alike. In this Article, I have provided the perspectives of two critical sets of actors in third-party search procedure, which show that internet technology companies do not carry out unitary, deliberatively determined strategies of either cooperation with, or resistance to, government surveillance. Instead, companies undertake a set of practices to cope with the practical

[301] E.g., Aleecia M. McDonald & Lorrie Faith Cranor, How Technology Drives Vehicular Privacy, 2 I/S: J.L. & Pol'y for Info. Soc'y 981, 1001–02, 1006, 1015 (2006); Carter Manny, Driven Data: Connected Cars and Privacy Law, 51 Bus. L. Rev. 35, 36, 46 (2018).

[302] E.g., Andrew Guthrie Ferguson, Digital Habit Evidence, 72 Duke L.J. 723, 753–58 (2023).

[303] Mark A. Hall, Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records, 95 Iowa L. Rev. 631, 643–44 (2010); Nicolas P. Terry & Leslie P. Francis, Ensuring the Privacy and Confidentiality of Electronic Health Records, 2007 U. Ill. L. Rev. 681, 714–16; Geoffrey Lightfoot & Tomasz Piotr Wisniewski, Information Asymmetry and Power in a Surveillance Society, 24 Info. & Org. 214, 216, 223–24 (2014); Konnoth, supra note 29, at 2184–86; Carrillo, supra note 29, at 1241.

[304] See Trump v. Vance, 140 S. Ct. 2412, 2420 (2020) (quoting 12 The Parliamentary History of England 693 (William Cobbett ed., London, T.C. Hansard 1812)).

difficulties arising from their work. I have also advanced the concept of knowledge misalignment to explain the nature of those difficulties and the practices that have developed among companies to manage such misalignment.

In addition to these empirical and theoretical contributions, I have identified important institutional implications of these practices for the evidence available to evidence seekers and the continuing operation of search procedure for internet evidence. Because judicial officers likely lack the capacity to oversee third-party search procedure for internet evidence in a meaningful and rigorous way, I have argued for the consideration of multiple institutional interventions to help ensure that company search and data production practices are visible, consistent, and tractable with respect to Fourth Amendment search procedure. Ultimately, decisions about whether to modify or intervene in the current system of acquiescence in the makeshift solutions imposed by company compliance staff is one that the public and its government representatives must decide. This Article has identified key insights into companies' practices that should be considered as part of that determination.

APPENDIX

Table 1. Research and Triangulation Interviews

	Companies	**Law Enforcement**
Research Interviews	20	27
Triangulation Interviews	8	5
Total	28	32

Table 2. Company Research Interviews

Company Label	Number of Interviews	Industry	Recruitment Method
1	4	Internet technology services	Cold: 1 Network: 3
2	2	Internet technology services	Cold: 2
3	1	Social media, networking	Niche: 1
4	1	Social media, networking	Network: 1
5	1	Social media, networking	Snowball: 1
6	1	Online storage, hosting	Snowball: 2
7	1	Online storage, hosting	Cold: 1
8	1	Online storage, hosting	Niche: 1
9	3	Online market	Network: 1 Snowball: 2
10	1	Online market	Cold: 1
11	1	Online market	Cold: 1
12	1	Online market	Cold: 1
13	1	Legal services	Network: 1
14	1	Legal services	Niche: 1
Totals			
14 organizations	20 respondents	Companies	Respondents
		12 companies 2 law firms	Cold: 7 Network: 6 Niche: 3 Snowball: 4

Table 3. Law Enforcement Research Interviews

Agency Label	Number of Interviews	Agency Type	Recruitment Method
1	3	Police Department	Cold: 3
2	2	Police Department	Cold: 2
3	1	Police Department	Cold: 1
4	2	Police Department	Cold: 2
5	2	Police Department	Cold: 2
6	1	Police Department	Snowball: 1
7	1	Police Department	Cold: 1
8	1	Police Department	Cold: 1
9	1	Police Department	Cold: 1
10	1	Police Department	Cold: 1
11	1	Police Department	Cold: 1
12	1	Police Department	Cold: 1
13	1	Sheriff's Office	Cold: 1
14	4	District Attorney's Office	Network: 2 Snowball: 2
15	1	District Attorney's Office	Cold: 1
16	1	State Investigative Agency	Cold: 1
17	1	Federal Investigative Agency	Cold: 1
18	2	Federal Prosecution Agency	Network: 1 Snowball: 1
Totals			
18 agencies	27 respondents	Agencies Municipal: 12 County: 3 State: 1 Federal 2	Respondents Cold: 20 Networking: 3 Snowball: 4

Table 4. Research Interview Details

	Companies		All Agencies	
Number of Research Interviews	20 respondents		27 respondents	
Recording	Recorded: Not recorded:	15 5	Recorded: Not recorded:	21 6
Format[305]	In person: Phone: Video: Written responses:	2 2 16 0	In person: Phone: Video: Written responses:	8 11 8 2
Interview Length (minutes)	Mean: Median: Range: Total:	105 86 30 to 256 2,100 (35 hours)	Mean: Median: Range: Total:	91 82 20 to 325 2,457 (41 hours)

[305] These may not add up to the total numbers of research interviews because some interviews were conducted through multiple formats.

Table 5. Sizes of Companies[306] and Agencies (Local and State)[307]

	Companies		State and Local Agencies	
Organization Size (employee count)	Fewer than 500:	0	Fewer than 10:	0
	500 to 1,000:	1	11 to 20:	1
	1,001 to 5,000:	5	21 to 50:	7
	5,001 to 10,000:	3	51 to 100:	4
	Over 10,000:	9	101 to 300:	8
			Over 300:	4
Department Size (employee count)	1 to 3:	4	1 to 3:	5
	4 to 10:	5	4 to 10:	4
	11 to 20:	4	11 to 20:	7
	21 to 50:	2	21 to 50:	3
	Over 50:	3	Over 50:	5

[306] These do not include outside counsel respondents.
[307] These do not include federal law enforcement respondents.

Table 6. Company Research Respondents[308]

	Frontline		Managers	
Number of Research Interviews	9 respondents		9 respondents	
Titles	Assistant, Analyst, Specialist: Lead, Counsel: Engineer:	3 5 1	Manager, Senior Manager: Senior Counsel: Director: General Counsel:	2 3 3 1
Years of Experience in Legal Process Compliance	1 to 2 years: 3 to 5 years: 6 to 10 years: Over 10 years:	3 4 2 0	1 to 2 years: 3 to 5 years: 6 to 10 years: Over 10 years:	2 2 3 2
	Mean: Median:	3.9 3	Mean: Median:	8 7
Previous Experience in Law Enforcement	Yes: No:	0 9	Yes: No:	3 6

[308] These do not include outside counsel respondents.

Table 7. Law Enforcement Research Respondents (Local, State, Federal)

	Investigators		**Prosecutors**	
Number of Research Interviews	22 respondents		5 respondents	
Titles	Detective, Agent, Inspector: Corporal, Lieutenant, Sergeant: Chief, Deputy Chief, Commander:	15 4 3	County: Federal:	3 2
Years of Experience in Law Enforcement	1 to 5 years: 5 to 10 years: 11 to 20 years: Over 20 years:	0 5 12 5	1 to 5 years: 5 to 10 years: 11 to 20 years: Over 20 years:	1 3 1 0