

ARTICLE

Symbolic ambivalence: how platform companies navigate contested law

Yan Fang 

Boston College Law School, Newton, MA, USA

Email: yan.fang@bc.edu

(Received 9 February 2025; revised 9 August 2025; accepted 26 October 2025)

Abstract

Organizations are often drawn into the contested work of criminal law enforcement. Through compulsory process and mandatory reporting laws, governments routinely conscript organizations such as hospitals, banks, and schools into assisting in surveillance activities whose legitimacy is socially contested. In recent years, conscription has been particularly pronounced with online platform companies, whose extensive collections of user data make them frequent sources of information and evidence for law enforcement agencies. How do actors in platform companies navigate compliance with such contested laws? While neoinstitutional theories of law emphasize how perceived compliance can protect organizational legitimacy, this article shows how perceived compliance with contested laws can also undermine it. Drawing on in-depth interviews with legal and operations staff for platform companies and law enforcement agents, this article explains how perceived compliance with contested laws can give rise to a legitimacy dilemma that organizational actors manage through *symbolic ambivalence*: compliance practices that signal both an organization's responsiveness to a law, as well as its independence from the aims, consequences, and institutions associated with the law. The article also suggests organizational and legal conditions that shape how platform actors engage in symbolic ambivalence. These findings extend neoinstitutional theory by showing that the relationship between perceived compliance and legitimacy is not straightforward, but contingent, and by explaining how organizational actors manage the legitimacy dilemma brought about by that contingency.

Keywords: Compliance; organizational legitimacy; platforms; policing

Introduction

Online platform companies are routinely conscripted into the enforcement of criminal law. These companies build Internet-based systems to facilitate transactions between different groups of users – for example, creators and viewers, or buyers and sellers – and collect substantial amounts of information about those users in the process (Cohen 2019; Van Dijck et al. 2018). They include companies such as Meta, whose social media applications connect people communicating with one another while providing advertisers access to those users (Van Dijck et al. 2018); Uber, whose application enables

passengers to request and pay for rides and deliveries from drivers (Rosenblat 2018; Van Dijck et al. 2018); and eBay, which provides online marketplaces for users seeking to buy and sell goods (Lehdonvirta 2022). In facilitating and mediating such transactions, platforms accumulate detailed records of user attributes and behavior, often becoming aware of criminal activities occurring through their services, such as harassment, fraud, human trafficking, and sexual exploitation of children (Citron 2014; Suzor 2019; Tyler et al. 2025).

As part of their responses to these criminal activities, companies have undertaken a variety of governance efforts. Some have established policies that prohibit such conduct and authorize the suspension or termination of accounts engaged in prohibited activities (Citron and Waldman, *forthcoming*; Gillespie 2018; Jiang et al. 2020; Pfefferkorn 2022; Tyler et al. 2025). Many have also established “trust and safety” teams that use companies’ extensive data collections to monitor potential wrongdoers, and to terminate accounts and prevent individuals from opening new ones (Denyer Willis 2023; Gillespie 2018; Jonas and Burrell 2019; Pfefferkorn 2022).

Platform companies are also routinely conscripted into public enforcement through compulsory process and mandatory reporting laws, which require companies to provide information and evidence about crimes, often those undertaken by their users (Bloch-Wehba 2021; Fang 2024). Because platforms facilitate large numbers of interactions between users and collect extensive information about those interactions and accounts, they possess data – communications, locations, and social connections – that are often relevant to criminal investigations and can thus help to identify potential wrongdoers and provide evidence for subsequent prosecutions. To respond to such legal obligations, companies have established law enforcement response teams that review and respond to search warrants seeking information about users’ identities and activities (Fang 2024).

While these law enforcement response teams enable companies to respond to their legal obligations, their conscription into criminal enforcement also creates legitimacy problems. On one hand, perceived compliance with conscriptive law can serve organizational legitimacy by signaling commitment to companies’ legal obligations. At the same time, such compliance can also undermine legitimacy when the laws themselves are socially contested – that is, when different segments of a company’s audience hold differing views about whether the law’s aims and consequences are just or effective.

A variety of circumstances make conscriptive laws contested. First, they facilitate surveillance – the gathering of “some form of data connectable to an individual” (Marx 2016). Surveillance is frequently controversial because it is understood to facilitate state monitoring of private communications; to reduce individuals’ autonomy and freedom to learn, speak, and associate; and to lack mechanisms for transparency and accountability (Richards 2013). Second, the particular substantive laws that conscriptive laws are used to enforce are sometimes also contested. Compulsory legal process may be used to gather evidence to enforce criminal laws prohibiting conduct ranging from fraud and homicide to the distribution of drugs, and, in some states, the provision of abortion access. Third, the government agencies that use conscriptive laws to aid their work – often, police agencies – are themselves the subject of significant public disagreement, even if the legitimacy of police appears to remain higher than that of other government institutions (Tyler 2023). This means that when companies respond to conscriptive laws, they do so in an environment where the legitimacy implications of

perceived compliance can be uncertain. How do actors in platform companies navigate such contested law?

This question remains underexamined in existing literature. Studies of platform governance recognize the legitimacy problems faced by companies and often criticize the efficacy and normative desirability of criminal legal institutions' influence on companies (Bloch-Wehba 2019; Caplan 2023; Dvoskin and Kadri, *forthcoming*; Musto et al. 2021), but have not inquired into how platform actors approach and understand their conscriptive obligations. While neoinstitutional studies of compliance offer insight into how organizations manage legitimacy conflicts between the aims of businesses and the aims of law (Edelman 2016; Edelman and Suchman 1997; Talesh 2009, 2012), they are of limited use in explaining how companies navigate conscription because they tend to treat perceived compliance as straightforwardly legitimacy-enhancing. This article shows that perceived compliance can operate not only to enhance an organization's legitimacy but also to weaken it. Drawing on in-depth interviews with legal and operations staff from platform companies and law enforcement agents, I show that when the legitimacy of a law is contested, organizational actors face a dilemma in which both perceived compliance – and perceived noncompliance – are understood as potentially reducing the organization's legitimacy with some audiences. I then show how organizational actors manage this dilemma through practices of symbolic ambivalence that signal both compliance with conscriptive laws and independence from formal law enforcement efforts.

Perceived compliance and organizational legitimacy

Organizational legitimacy is the “generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate, within some socially constructed system of norms, values, beliefs, and definitions” (Suchman 1995: 574). State institutions and laws play an important role in organizational efforts to maintain legitimacy because they provide institutionalized rules and practices – attention to which can help an organization appear right and appropriate (DiMaggio and Powell 1983; Meyer and Rowan 1977). In other words, they establish “official” and “authoritative” models and criteria for how organizations should be arranged and how actors within organizations should behave (Meyer and Rowan 1977: 347). And when entities organize themselves in ways consistent with these legally sanctioned models and criteria, organizations can signal that they are legitimate social actors (Scott 1998).

Neoinstitutional theories of law have elaborated on the relationship between organizational legitimacy and the legal environment, showing how organizations create internal structures that simultaneously appear to satisfy legal requirements and serve organizational interests. Lauren Edelman's work on organizations' perceived compliance with employment discrimination laws theorizes this process. When faced with new civil rights laws that sought to constrain managerial prerogative by mandating equality in the treatment of employees, organizations created internal grievance offices and procedures that looked like the “formal protections of due process rights” of the “public legal order” (Edelman 1990: 1409). Because public legal processes are “a basic and well-institutionalized feature of a legitimate normative order” (Edelman et al. 1999: 416), internal grievance processes could operate as visible signals of the organization's fair treatment of its workers (Edelman 1990, 1992, 2016).

A key condition underlying the legitimizing capacity of compliance signaling is that the laws in question are broadly viewed as having socially desirable aims and consequences. Many legal endogeneity studies examine organizational responses to laws that enjoyed substantial normative support at the time of study – such as civil rights, consumer protection, and privacy regulations (Edelman 2016; Talesh 2009, 2012, 2015; Waldman 2021). As Edelman points out, when a “law enjoys considerable societal support” or “provides the public with new expectations or new bases for criticizing organizations,” “apparent noncompliance is likely to engender loss of public approval” (Edelman 1990: 1406). Symbolic compliance thus enables organizations to maintain legitimacy by undertaking actions that demonstrate attention to law while preserving sufficient flexibility to protect organizational prerogative to prioritize nonlegal goals (Edelman 2016: 31).

Not all laws, however, enjoy broad or consistent support. Organizations operate under multiple, sometimes conflicting, institutional logics that prescribe different sets of appropriate practice (Friedland and Alford 1991; Pache and Santos 2010; Royston et al. 2011; Thornton et al. 2012), some of which may conflict with legal principles and practices. Healthcare organizations and providers, for example, can operate at the intersection of logics originating in law, medicine, and family, each of which establishes different criteria for appropriate organizational practice (Chiarello 2015, 2023, 2024; Heimer 1999). Even within the domain of law itself, organizational actors navigate laws and practices whose underlying priorities and principles vary (Heimer 1999; McPherson and Sauder 2013). When responding to contested laws, organizations and their actors may not necessarily regard perceived compliance with such laws as increasing legitimacy.

Perceived compliance as a contingent source of legitimacy

When a law lacks broad social acceptance, organizational actors may in fact view perceived compliance as *undermining* legitimacy. This possibility gives rise to a distinct dilemma for these actors because both perceived compliance and perceived noncompliance are understood as having potential legitimacy costs. In classic neoinstitutional studies of law, organizational actors struggle with the dilemma of meeting both legal and business logics, whose imperatives conflict (Edelman 2016; Talesh 2009, 2015; Waldman 2021). Where the legitimacy of a law itself is contested, however, organizations’ dilemma instead arises from the fact that both perceived compliance and perceived noncompliance with the contested law can reduce an organization’s legitimacy. Organizational responses to this dilemma will vary depending on how organizational actors assess the legitimacy of perceived compliance with the contested law.

Existing research suggests that both the characteristics of organizations and the law at issue will shape how organizational actors understand the legitimacy implications of perceived compliance in such cases. At the organizational level, the newness of the organization’s field is one condition that may shape how actors assess whether perceived compliance would enhance or reduce organizational legitimacy. Fields are “those organizations that, in the aggregate, constitute a key recognized area of institutional life” (DiMaggio and Powell 1983: 148). Fields are marked by shared understandings about the purposes and practices of organizations within them – understandings

that shape whether actors may view compliance with a contested law as serving organizational legitimacy or as undermining it. In fields that are older and more heavily regulated, such as healthcare or banking, organizational responses to formal laws may be more routinized and institutionalized (Scott 1998), making perceived compliance a more reliable source of legitimacy. Organizations in newer or emerging fields, in contrast, may lack certainty in the institutional rules defining legitimate activities (Greenwood et al. 2011; Kluttz and Fligstein 2016). Organizations in such fields may cultivate legitimacy by distinguishing themselves from conventional organizational forms, not necessarily by demonstrating adherence to established practices.

In addition to its field, an organization's features may also shape its actors' assessments of the legitimacy of perceived compliance. First, organizational size may shape the range of audiences under consideration (Adediran 2026). In particular, larger – and “leading” – organizations may face more scrutiny by audiences such as the media, regulatory bodies, and social movement organizations (Bartley and Child 2014; Deephouse 1996), increasing the likelihood of encountering audiences with divergent views on contested laws. Second, there is the nature of the organization's business – including whether it is consumer facing and the potential severity of harms associated with its services. Well-recognized organizations may be more vulnerable to reputational sanctions (Bartley and Child 2011), as are organizations whose services carry potential for significant injuries to customers and the public (Vergne 2012).

The contestedness of the law at issue may also shape how organizational actors assess the legitimacy implications of compliance. A law may be contested when its underlying policy objectives, implementing actors, or enforcement consequences lack acceptance among some audiences. For instance, some laws may be contested because they address substantive matters that generate significant social disagreement, such as reproductive autonomy or immigration legalization (Luker 1984; Song and Bloemraad 2022), or that impose obligations that conflict with the norms and logics of established professions (Chiarello 2015; Heimer 1999). Laws may also be contested when the authorities who create or enforce them, or the procedures through which they are made or implemented, are viewed as illegitimate (Tyler and Fagan 2008; Verma 2015). For example, organizational actors may question whether perceived compliance will enhance organizational legitimacy when they view enforcement agents to be unreasonable or incompetent (Bardach and Kagan 1982; Gray and Silbey 2014). When laws are contested in these ways, organizational actors face uncertainty about the legitimacy implications of compliance. Perceived compliance may signal responsibility to some audiences while signaling complicity with unjust or harmful policies to others. Conversely, perceived noncompliance may be interpreted as principled resistance by some audiences and as unlawful defiance by others.

The legitimacy dilemma becomes particularly acute with conscriptive laws that enlist organizations into criminal enforcement. In contrast to many forms of organizational regulation, which are often understood as promoting individual and social welfare, there is more disagreement about the normative desirability of conscriptive laws (Ayling and Grabosky 2006; Gilboy 1998). Such laws – which include laws requiring banks to report large or unusual financial transactions (Ball et al. 2015; Byrne 1993; Levi 1991), telecommunications carriers to assist in wiretapping phones (Boustead 2016; Nunn 2008), teachers to report potential child abuse (Gallagher-Mackay 2014), physicians and nurses to report gunshot wounds or elder abuse (Song 2021), and

pharmacists to refuse suspicious prescriptions (Chiarello 2015, 2023, 2024) – are routinely criticized as mechanisms of surveillance, especially when they further draw marginalized individuals into the criminal legal system (Brayne 2014; Brayne et al. 2023; Gustafson 2009). By compelling organizations and individuals to report and produce evidence of suspected wrongdoing, these laws not only force organizations to interact with law enforcement agencies and to assist in the enforcement of criminal laws, both of which may be contested, but also transform organizations into participants in state enforcement efforts against individuals. At the same time, however, perceived noncompliance carries its own legitimacy costs – particularly when investigations concern crimes whose prohibition is more broadly accepted.

To manage this legitimacy dilemma, organizational actors may undertake compliance practices that signal both compliance with conscriptive law and independence from law enforcement efforts. Existing theory, however, does not sufficiently explain how organizations manage this type of legitimacy dilemma because it tends to treat perceived compliance as enhancing legitimacy. The concept of symbolic structures or symbolic compliance typically describes compliance activities that “symbolically demonstrate attention to law” (Edelman 2016: 31). As such, when organizational actors undertake practices of symbolic compliance, they signal one principal message: that the organization is responsive to the aims of the law at issue. The concept of symbolic compliance does not capture the second message that an organization may also signal when responding to contested law: that it is independent – and thus does not necessarily support – the aims, consequences, or associated institutions of the law at issue.

I introduce the concept of symbolic ambivalence to describe compliance practices undertaken by organizational actors that signal these distinct messages. Symbolic ambivalence has two defining elements. The first element operates as the concept of symbolic compliance does, and it consists of compliance practices that signal an organization’s responsiveness to the aims of a law, irrespective of whether those practices substantively achieve the aims of that law. The second element is also symbolic, in that it signals a message about the organization’s response to a law. However, that second message is distinct from the message of symbolic compliance because it signals the organization’s *independence* from that law. This element of symbolic independence is critical for understanding how organizations navigate the legitimacy dilemma arising from compliance with contested law because it explains how organizational actors can also distance the organization from the contested law.

Platform companies as a case study

Online platforms provide a compelling case for examining how organizations maintain legitimacy when navigating conscriptive law. Historically, platform companies have had a contested relationship with state authority. During the early internet era, libertarian and techno-utopian ideals corresponded with companies’ framing of their services as neutral intermediaries rather than editorial gatekeepers (Barbrook and Cameron 1996; Gillespie 2010; Kosseff 2019; Suzor 2019). This framing enabled platforms to avoid legal obligations that governed existing media organizations, including through successful litigation of Section 230 of the Communications Decency Act to broaden companies’ immunity from liability for materials posted – and conduct

undertaken – by platform users (Citron 2023; Kosseff 2019). Facebook’s founding ethos of “move fast and break things” and Uber’s strategy of entering markets without regulatory approval also exemplify how companies’ distancing from existing law and institutions initially helped them succeed (Collier et al. 2018; Taplin 2017).

But as people brought “all of social life” online (Fourcade and Healy 2024: 65) and platform companies grew much larger, maintaining such a stance of independence from state authorities and the law become more difficult. In particular, the capacity of platform services to facilitate all kinds of social problems made them both attractive targets of regulation and valuable sources of information and evidence for government authorities. For example, as state actors recognized the proliferation of child sex abuse material (Cullen et al. 2020; Farid 2018; Keller and Dance 2019), cyber harassment and stalking (Citron 2014; Marwick and Caplan 2018; Soneji et al. 2014), and terrorist and extremist activities (Doeck 2022; Mitts 2025), there were more frequent interactions between platforms and wide-ranging state and legal institutions, including law enforcement agencies, legislative bodies, and regulatory agencies. With this expansion in the scope and frequency of interactions with state actors, the legitimacy stakes of companies’ conscription also becomes more complex.

In some ways, platform companies’ efforts to distance themselves from state authorities intensified following public disclosures of their role in national surveillance programs. In 2013, former National Security Agency contractor Edward Snowden revealed that US intelligence agencies had conducted extensive, secretive surveillance, often using data from major platform companies (Lyon 2015). These revelations subjected companies to intense criticism from US and international media, civil liberties groups, and government officials for their role in the mass surveillance of citizens and noncitizens (Bauman et al. 2014; Weber 2019). Subsequently, numerous platform companies publicly adopted more adversarial stances toward government data requests, including through the publication of transparency reports that disclose the volume of search warrants, subpoenas, and other compulsory legal process demands received by companies, and the issuance of “warrant canaries” – statements in transparency reports affirming the absence of national security information demands that, if removed, would signal receipt of such demands (Reid et al. 2024; Wexler 2014). In addition to these statements, some companies touted their protection of user data against state intrusion as a central aspect of their organization’s identity – most publicly, in 2016, when Apple challenged a court order obtained by the Federal Bureau of Investigation to unlock an iPhone used in a mass shooting in San Bernardino, California (Rozenshtein 2018; Weber 2019).

At the same time, defying legal orders carries its own legitimacy costs. Ignoring valid warrants and orders risks characterizing companies as lawless or even complicit in facilitating wrongdoing – a characterization that can be damaging to organizational legitimacy, both externally and internally. Such a characterization may be especially problematic for large, consumer-facing companies subject to growing scrutiny (Zittrain 2023; Zuckerman and Rajendra-Nicolucci 2023). Indeed, in 2018, the US Congress passed the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), which narrowed Section 230 immunity for platforms that knowingly promote or facilitate sex trafficking (Albert et al. 2021; Citron 2023). Outside the United States, the European Union’s Digital Services Act, which came into effect in 2022,

imposed affirmative duties on companies to inform law enforcement in member states of crimes involving threats to life or safety (Bender 2025).

These developments place platforms in a complex legal environment. Perceived noncompliance with conscriptive demands can signal obstruction, complicity, and a lack of organizational commitment to protecting user safety, thus decreasing legitimacy with law enforcement and regulatory audiences, as well as some consumers and other audiences. At the same time, perceived compliance can erode platforms' legitimacy among audiences that reject the efficacy and normative desirability of government information gathering. Given these conflicting implications for legitimacy, how do platform actors navigate contested laws?

Data and methods

I approached this question by seeking the perspectives of two sets of actors: workers at platform companies who respond to conscriptive obligations and law enforcement investigators who seek information and evidence from platform companies. Interviews with the former reveal how platform actors assess conscriptive demands and how these perceptions shape their decisions and routine compliance responses. Interviews with law enforcement provide an external perspective on company actors' practices, thereby offering indirect insight into how company actors navigate conscriptive laws. To identify such respondents, I used multiple sampling strategies: random, convenience, niche, and snowball.

For law enforcement, I focused on investigators who were sworn officers for municipal police departments or county district attorneys' offices. I also included county prosecutors, who do not necessarily prepare search warrants but may still play a role in reviewing applications. I also focused on investigators and prosecutors within California agencies, which helped control for variations in state law – such as criminal procedure and privacy laws – that could affect how agents draft warrants and, in turn, how companies respond to them. At the start of this study, California was the only state requiring the annual public release of data on a subset of search warrants issued to companies, which enabled random sampling of companies and law enforcement agencies. I thus drew a sample of agencies from a public dataset of search warrants released by the California Department of Justice (California Department of Justice Data Portal 2016–2020) and a federal dataset (US Department of Justice Bureau of Justice Statistics 2016), which yielded a combined sample of 71 agencies. I contacted the police chief or the sheriff at each agency to request permission to interview one or two investigators. 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 random sample. When conducting interviews, I asked respondents if they would share information about the study with colleagues.

To identify companies, I drew a random sample of fifty-four US-based companies from the California Department of Justice dataset. I then used a similar combination of cold outreach, convenience sampling, niche sampling, and snowball sampling to identify individuals to contact. For cold outreach, I used LinkedIn Premium to search for employees at these companies whose profiles included keywords such as “warrant,” “law enforcement,” and “safety.” I reviewed each profile and identified those whose roles appeared most relevant. I sent LinkedIn messages to one to three individuals

per company, focusing on frontline staff and managers when they could be identified. For the other types of sampling, I contacted people in my professional network who worked at the sampled companies; attended legal conferences, talks, and panels where I met potential respondents; and asked respondents if they would contact colleagues who may be interested in the study. Again, this combined approach involved reaching out to individuals from companies outside the random sample, including outside counsel who advise companies on compulsory legal process and mandatory reporting.

When approaching potential respondents, I first held an introductory phone call or video conference to explain my research. Some potential company and law enforcement respondents were reluctant to discuss their work, which is often under public scrutiny. To address the possibility that respondents' hesitancy and the topic's sensitivity might lead some to omit details, I also conducted triangulation interviews. While research participants agreed to have their responses used in publications and presentations without attribution to protect their anonymity, the triangulation interviews provided comparison points for the research interviews; they have not been quoted or paraphrased in this article.

In total, I conducted forty-seven in-depth interviews: twenty with platform staff and twenty-seven with law enforcement agents. I also conducted thirteen triangulation interviews: eight with platform actors and five with law enforcement. Both the research and triangulation interviews were conducted between 2019 and 2023 in a semistructured format. This approach permitted a set of planned questions as well as flexibility to explore additional themes that arose during the interviews. My interview guide asked respondents to discuss two recent warrants they had either drafted or reviewed. This item was followed by questions such as, "Do questions arise when you are reviewing a warrant? Can you give me an example?" This set of questions encouraged respondents to elaborate on their experiences and allowed me to probe specific aspects of their answers. They also led both research and triangulation interview respondents to discuss mandatory reporting and emergency information requests. These discussions were followed up by questions such as, "How has your work changed over time? What have you found rewarding about the work? What have you found difficult?" These broader questions often prompted respondents to reflect on their values and the challenges they faced in their work.

I used MaxQDA to code the transcripts and notes for the research and triangulation interviews iteratively during the analysis. During early phases of coding, I focused on descriptive coding to categorize the examples that respondents discussed on the basis of labels such as case type, data sought, and views toward the request. I also coded for principles, ideas, and values that people discussed, focusing on the language that respondents used to describe their roles, work, and interactions. Finally, I coded each respondent's background, including demographic information, role within the organization, and length of time on the job. I wrote analytic memos to develop conceptually oriented codes and subcodes, identifying potential relationships between them by consulting relevant literature and employing inductive and abductive reasoning (Glaser and Strauss 1967; Timmermans and Tavory 2012). In later coding phases, I recoded the interview transcripts and notes using conceptual coding categories, refining codes and subcodes, and identifying topics and subtopics. This stage focused on exploring potential relationships between codes and identifying confirmatory examples and outliers. MaxQDA's analytical tools were particularly useful for comparing subsets of

respondents, such as those who participated in the research versus those who participated in triangulation interviews. I did not find systematic differences between the information reported during each of those types of interviews. For the analysis below, I paraphrase, quote, and excerpt only from the forty-seven research interviews. All individual names, organizational names, and other personally or organizationally identifying information have been removed, consistent with protocols approved by the UC Berkeley Committee for the Protection of Human Subjects, under CPHS Protocol Number 2019-10-12590, and the Boston College Institutional Review Board, under IRB Protocol Number 25.124.01e.

Platform actors: Law enforcement response, trust and safety

The company respondents worked for platforms whose services spanned email, messaging, search, document and media hosting, social media and networking, online marketplaces, dating, ride-hailing, and network hospitality. Most worked for relatively larger companies: five worked for companies with 1,000 to 5,000 employees, and twelve worked for companies with more than 5,000 employees. Among these respondents, there were two main sets of actors: those who primarily respond to law enforcement demands and those who also have trust and safety responsibilities.

Of the twenty company respondents, thirteen worked on teams referred to as “law enforcement response team,” “law enforcement operations,” or “subpoena compliance” (collectively, law enforcement response or LER). These teams were typically situated within legal departments, and ranged in size from two to over one hundred employees. On these teams, LER staff’s responsibilities consisted primarily of responding to search warrants and other legal process requests. Of these LER respondents, nine were lawyers, with titles including “counsel” and “director.” Four were nonlawyer managers or frontline personnel with titles including “assistant” and “manager.” Among the LER respondents, six had experience working at more than one platform company.

Seven company respondents had substantial trust and safety (T&S) responsibilities, including two with both T&S and LER responsibilities. Companies use the term T&S to refer to more proactive practices aimed at protecting online platforms and digital environments from antisocial user activities, such as fraud, abuse, harassment, and child exploitation (Citron and Waldman, [forthcoming](#); Tyler et al. 2025). The phrase has been traced to eBay, where “trust” referred to confidence among users and confidence in the company; it later became a common term for teams focused on protecting users from harmful conduct and experiences, including by setting policies and procedures, conducting investigations, and designing systems to implement set rules (Boyd, 2002; Trust & Safety Professional Association, [n.d.](#)). These respondents held titles such as “counsel,” “director,” “manager,” “specialist,” and “engineer,” and worked on teams of one to over fifty employees. Five had experience at multiple platform companies, and two were attorneys. While some T&S respondents worked as part of engineering, product, or operations teams, two sat within legal departments.

The legitimacy dilemma

In the next sections, I use data from interviews with LER and T&S respondents to explain how platform actors navigate contested laws by undertaking actions that

signal both responsiveness to legal mandates and independence from law enforcement efforts. The first two sections focus on how the legitimacy dilemma manifests and is experienced by platform actors conscripted into criminal enforcement. The subsequent sections turn to how and when actors undertake practices of symbolic ambivalence that signal distinct messages about organizational compliance.

Assessing perceived compliance as reducing legitimacy

In everyday work, the legitimacy dilemma is often triggered by search warrants. Search warrants are judicial orders authorizing law enforcement agents to search a person or premises. Under the federal Electronic Communications Privacy Act of 1986 (ECPA), companies are prohibited from disclosing users' information, records, or communications unless compelled to do so by a warrant, subpoena, or court order directing their production (Kerr 2004). The California Electronic Communications Privacy Act (CalECPA), is more stringent, requiring a search warrant for law enforcement to access communications information, including metadata (Freiwald 2018). When a search warrant arrives at a platform company, LER staff typically receive an order identifying the account(s) subject to search and the items to be seized, the applicable statutes and the offenses under investigation. LER staff then interpret the warrant's legal language in terms of the company's own data holdings, mapping sometimes broad requests onto specific account identifiers, logs, content types, and time ranges (Fang 2024).

When describing their work responding to such legal demands, respondents expressed concerns about how perceived compliance might affect two forms of organizational legitimacy: moral legitimacy and pragmatic legitimacy. Moral legitimacy concerns whether organizational actions conform to societal norms and promote the collective good, regardless of their potential for benefitting particular audiences instrumentally (Suchman 1995). In contrast, pragmatic legitimacy concerns whether organizational activities provide tangible benefits or advantages to specific audiences (Suchman 1995). While both forms were at issue in platform respondents' assessments, the distinction between them did not matter analytically. Whether respondents reported concerns about moral or pragmatic legitimacy, they faced the same uncertainty about whether perceived compliance would enhance or reduce that legitimacy.

In terms of moral legitimacy, company respondents described compliance with warrants as worrisome because doing so could be seen as infringing on platform users' privacy. Several respondents emphasized that account data should be protected – meaning that the data should not be readily turned over to the government (Counsel, July 2021; Legal Assistant, October 2021). Respondents' concerns about the legitimacy implications of providing responsive data were particularly salient when they discussed warrants that sought data using a long list of data fields or that seek “all” records or data from “all” company products, which, to them, suggested that law enforcement may be trying to obtain data that agents were not entitled to or that were unnecessary for their investigations (Legal Director, November 2021). As one legal assistant explained, such broad warrants were “fishing” requests because the officers likely had “a sense that a crime had been committed, they established probable cause” but were also “looking for other crimes or other things that may have happened in different products and services” (Legal Assistant, February 2022).

Some also assessed the possibility that law enforcement could end up targeting the wrong user, which would reflect poorly upon the company producing the data. One respondent reported worrying that if law enforcement relied solely on information from companies and lacked additional evidence, officers could end up arresting an innocent person (Legal Assistant, September 2021). Another respondent discussed the risk that law enforcement may target marginalized groups: “Law enforcement has not moved the needle on how they treat people with mental issues, ... or they don’t believe the LGBTQ+ community, or they discriminate against their color ... We’ve seen [cases] where law enforcement has requested information from companies where it is in fact to criminalize that person – whether that be [because] they have some sort of mental illness, or they have suicidal ideation, or they are part of [the] LGBTQ+ community” (Director, April 2022). These reports suggest that respondents viewed perceived compliance with demands focused on minority and vulnerable individuals as carrying potential moral costs for legitimacy.

In addition to considering the implications of compliance for users’ safety and privacy, company respondents also reported concerns rooted in pragmatic legitimacy. These concerns arose when respondents discussed how some law enforcement agents lacked basic understandings of the types of data their companies hold or basic knowledge of what to do with the produced information. As one legal director explained, “Oftentimes, [law enforcement] overestimate the technical abilities that companies have – they oversimplify how systems work” (Legal Director, November 2021). Another director explained that, in some cases, the officer at the other end of the phone did not know how to use information provided by the company to locate the person likely in their jurisdiction. According to that director, “every person that works in this space has an endless number of stories of how, candidly, dumb law enforcement can be when they are asking for things that they cannot have or when they have no idea how your service works” (Trust and Safety Director, March 2021). Such interactions led platform respondents to question whether law enforcement was competent at gathering internet evidence and to doubt whether compliance would be seen as effective in investigating crimes or preventing people from being harmed.

Alongside law enforcement effectiveness, company respondents described another pragmatic risk associated with both perceived and substantive compliance: A thorough production of data in response to demands could expose conduct on their platforms or aspects of their data management to unwanted scrutiny from lawmakers and regulators. Respondents emphasized that they feared engaging with law enforcement because their responses might reveal problems on their platforms that their companies were not ready to publicly acknowledge. One in-house attorney noted that any request could lead to the company being investigated (Counsel, March 2022). Uber, for example, has been publicly criticized for having “ulterior” motives for failing to produce records in response to a search warrant in an investigation of sexual assault involving a driver with Uber (Gartrell and Kendall 2017), which could lead to regulatory interventions regarding the safety of its services (Steel 2025). Platform respondents were thus aware that complying with law enforcement requests could expose information that could lead to their companies being investigated or regulated.

Numerous respondents expressed an awareness of the visibility of companies to journalists and advocacy organizations. One attorney lamented that companies were consistently – and inaccurately – portrayed in the media as an “arm of law

enforcement” (Counsel, March 2022). Another reflected, “[j]ournalists are really terrible at explaining how legal process works and how governments or civil litigants even are able to request data from companies and what responsibilities companies have under the law” (Counsel, July 2021). In addition, between 2011 and 2017, a prominent privacy advocacy organization, the Electronic Frontier Foundation, issued annual “Who Has Your Back?” reports that evaluated companies’ policies on compulsory process demands using star ratings (Cardozo et al. 2016; Electronic Frontier Foundation 2011, 2012, 2013, 2014, 2015; Reitman 2017). One outside counsel remarked that for a time, clients cared a great deal about getting stronger privacy ratings, often asking: “[W]hat do we have to do to get our star?” (Outside Counsel, November 2021). While respondents recognized that the vast majority of company responses to conscriptive demands were not visible to outsiders, they were also aware that some demands – for example, those involving new types of information or more high-profile crimes – could receive more attention (Safety Manager, November 2021; General Counsel, September 2022).

In addition to potential external audiences, respondents also sought to manage the legitimacy implications of perceived compliance with internal audiences. One manager explained:

Our team is associated with being the law enforcement team. And in the last two years, there’s been some negative media around law enforcement and their practices. And so I think often we’re having to work through that ... That’s where I mentioned bringing different members of the team to different meetings, to bring different perspectives in some ways, to disarm that perception of our team ... because of some of the public perceptions and facts that are out there. (Safety Manager, November 2021)

Because their team is associated with contested law enforcement agencies – and contested law enforcement practices – this manager took efforts to appear objective and “disarm” that perception. Other respondents discussed the particular importance of appearing neutral to colleagues on engineering or product teams who were not familiar with companies’ conscriptive obligations under the law, but whose assistance is needed to build tools necessary to query, retrieve, and produce data to authorities. One legal assistant said that “the technical questions weren’t difficult [for the engineers],” but “the context is what they were most nervous about”: “Because as soon as you say national security or federal government or things like that, they’re like, ‘[W]hoa, whoa, whoa!’” (Legal Assistant, October 2021). To reassure such colleagues, she would explain that companies were required to provide such information under the law: “[I]f you want to read it yourself, here’s the code, here’s the sections, here’s the legislation.”

Assessing perceived noncompliance as reducing legitimacy – and perceived compliance as enhancing legitimacy

Platform respondents also recognized that perceived noncompliance carried its own legitimacy costs. As one legal director explained, demonstrating “integrity” was an important part of his work: “[I]f a company is constantly late in responding to legal

process, or is incomplete in responding to legal process, or turns over the wrong data ... or is just obstinate for no reason, that is a great hindrance ... because it just looks like a bad actor and isn't being responsible to the laws that are on the books - isn't being consistent with its own principles" (Legal Director, March 2023). In other words, perceived noncompliance – including delayed or incomplete compliance – could weaken organization legitimacy by making companies appear obstructive or negligent. This concern suggests that some level of responsiveness was thought necessary to maintain organizational standing, even when actors worried about the risks of fuller compliance.

Beyond avoiding potential legitimacy costs from perceived noncompliance, perceived compliance with conscriptive demands can also help to enhance organizational legitimacy. This can occur in a few ways. Sometimes, agents provide more facts about their investigation, allowing company staff to develop a better understanding of the case giving rise to the warrant. One respondent explained that he sometimes sought "context" from agents about their cases, including why investigators thought the company's users were involved (Investigations Specialist, December 2021). Officers also discussed sharing information about cases – especially when attempting to persuade LER staff to prioritize responding to a particular warrant (Detective, September 2022; Sergeant, September 2022). As staff interact with officers and learn about cases, they may come to want to assist the officer in identifying or finding evidence related to the wrongdoing or wrongdoer.

In addition, both in the course of producing data in response to law enforcement demands and in undertaking companies' own proactive monitoring or investigation of user wrongdoing, platform actors may become acutely aware of and concerned about the harm and abuse undertaken by some platform users, which can include physical violence. As one project manager explained, her job made her aware that "people do horrible things to people and take photos, and to babies and animals ... [It] opened my eyes to just the scale of how bad humanity could be, and that this platform enabled it" (Product Manager, July 2021). A manager similarly reflected, "It's almost like watching the bad parts of the news all day long. You're seeing the requests ... it's really in a lot of cases, a description of a very troubling, horrible experience or incident" (Safety Manager, November 2021). As platform actors become more aware of this conduct, their assessment can shift – viewing law enforcement demands as more morally legitimate and, correspondingly, compliance as capable of enhancing organizational legitimacy.

Respondents' work reporting child sexual abuse material (CSAM) plays a substantial role in shaping this perspective. Federal law requires companies to report known or suspected instances of such exploitation to the National Center for Missing and Exploited Children (NCMEC), a nonprofit organization that functions as a legally authorized clearinghouse for CSAM reporting (Cullen et al. 2020). CSAM refers to any visual depiction of sexually explicit conduct involving a minor (18 U.S.C § 2256). After reviewing a company's report, called a CyberTipline report or "CyberTip," NCMEC typically forwards it to a jurisdictionally appropriate criminal law enforcement agency for potential investigation. On the basis of the CyberTip and potentially other evidence, investigators may seek a search warrant naming the reporting company to compel additional information or records relating to the report (Grossman et al. 2024).

Respondents' assessments of compliance in child exploitation cases as morally legitimate were reflected in their descriptions of their work. As one respondent put it, "If there's a concern that there is a child at risk and the information provided is going to help save the child, they're going to do it on an emergency" (Legal Director, March 2023).

Indeed, many respondents used the same language as law enforcement when referring to the identification and punishment of users engaged in wrongdoing. For example, law enforcement respondents described their work as catching "bad guys" who break laws and hurt others. As one detective explained, "We go out and serve that search warrant, and [the] bad guy goes to jail, and we get the evidence that we need. That's extremely satisfying. That's why I do the job." (Detective, September 2022). Similarly, some company respondents prioritized catching "bad actors" – users who use company services to cause harm to others. Common examples included adults attempting to solicit minors for sexual exploitation, as well as sellers trying to defraud purchasers. As one legal assistant reflected, "At the end of the day, it's 'Hey, did we help keep someone safe? Did we put a bad guy, you know, behind bars?' To me, that's the value there" (Legal Assistant, September 2021).

The assessment of perceived compliance as enhancing legitimacy was also salient when respondents discussed providing information to law enforcement in emergency situations. Emergency requests are efforts to obtain user communications or records in situations of imminent danger to a person. Under ECPA and CalECPA, companies may disclose communications and records to law enforcement without a warrant if the provider, in good faith, believes that an emergency involving the danger of death or serious physical injury requires immediate disclosure (Freiwald 2018; Kerr 2004).

Respondents reported two kinds of emergency situations that typically prompt interaction with criminal law enforcement. First, law enforcement agents sometimes reach out to companies with reports of an imminent danger – such as bomb threats, abductions, active shootings, and threats of suicide – in which they believe the platform has information about particular users, such as their phone number, home address, or IP address, which might aid in locating an individual or facilitating a rapid response. Second, on occasion, platform actors may proactively contact law enforcement about potential threats they have internally discovered on their platforms (Legal Assistant, September 2021), or coordinate with agents about the timing and logistics of an arrest that occurs while a user is using a company's services (Counsel, March 2022). Several respondents explained that one of the most meaningful parts of their work was to intervene to stop wrongdoers and save people's lives. One investigations specialist explained, "It felt very impactful, the ability to connect my work to real deterrence of bad actors, actually resulting in prosecution" (Investigation Specialist, November 2021).

In cases where respondents viewed compliance with conscriptive demands as morally legitimate, some even characterized themselves as occupying roles similar to those of law enforcement. One manager explained, "I do something that's mission-driven that has an impact on people's lives in the world and at this company" (Safety Manager, October 2021). He suggested that for some of his staff who had previously served as officers, they saw their work inside companies as a continuation of law enforcement careers: "I think a lot of our team is very connected to that same mission. Even the people [previously] in law enforcement feel that they could help save

lives more by working in this job than they could have in public service.” A director also compared their work to that of police agencies: “With more complex law enforcement response teams, you start running your own [police department] – inherently, trust and safety is a platform’s police department of sorts” (Trust and Safety Director, March 2021). Taking actions to facilitate the identification and arrest of “bad actors” or prevent suicides reinforced respondents’ assessments that compliance efforts in these cases could serve moral legitimacy by signaling attention to collective safety and the protection of vulnerable users.

Respondents’ assessments that compliance could enhance legitimacy extended beyond moral concerns. Some respondents also characterized perceived compliance as pragmatically legitimate – in that assisting law enforcement in the investigation and prosecution of bad actors could help platforms become safer, and thus attract more users. That director explained, “[A company cannot] throw someone in jail. When someone is in jail, they can be put there forever. But when the platform bans someone, that person can still join or sign up again” (Trust and Safety Director, March 2021). Thus, “[t]he only way to get rid of them [bad users], sort of totally, is to cooperate with the law.” Another respondent emphasized the commercial benefits of perceived compliance, stressing that “keep[ing] our community safe” was a top goal because “[i]f we’re able to pull that person off our community,” that could also help remove “a barrier of entry” for potential and existing customers (Director, April 2022). In other words, assisting law enforcement can help companies to protect their services and to gain and retain users for their services.

Symbolic ambivalence as a response to the legitimacy dilemma

Given these crosscutting assessments of perceived compliance, platform actors face a distinct dilemma: perceived compliance can both enhance and erode organizational legitimacy. To navigate this dilemma, organizational actors engage in symbolic ambivalence – compliance practices that signal both responsiveness to legal mandates and independence from law enforcement efforts.

User-notification practices illustrate these responses particularly well. Under ECPA and CalECPA, companies are permitted to notify users of receipt of a warrant if no accompanying court order bars disclosure. Such notifications concern investigators because they can alert those users – who may be suspects, victims, or third parties – about the existence of the investigation. This may lead the user to switch services or delete account information, destroying potential evidence or leads. Thus, when officers apply for search warrants, they often also seek a court order prohibiting companies from notifying affected users of the warrant for a certain period of time. During interviews, platform and law enforcement respondents alike reported that companies typically comply with court orders explicitly prohibiting such notifications (Agent, November 2019; Detective, March 2021; Outside Counsel, October 2021; Legal Director, November 2021). Such compliance with no-notice orders signals companies’ responsiveness to legal mandates.

Platform actors, however, also engage in a related set of practices that signal independence from law enforcement: the closure of user accounts. While actors reported complying with no-notice orders, they also reported shutting down or suspending accounts – practices that could have the practical effect of notifying users anyway.

Both platform and law enforcement respondents reported that when company staff review a warrant relating to a particular account and, in the course of producing responsive data, see that the account has engaged in conduct that violates the company's terms of service or other user policies, the reviewer may independently shut down the account to stop the conduct – even despite being asked by law enforcement to keep the account open:

A lot of times, when [law enforcement] send in the search warrant, they will either include a nondisclosure order, and sometimes they would also include a request to keep the account open. We had a policy of not doing that ... the position that the company always took was we're not going to continue to allow abuse on our platform at the request of law enforcement just because they have this investigation going on. (Legal Assistant, February 2022)

Law enforcement respondents were aware of this practice and expressed concerns that account terminations and suspensions could alert accountholders that their activities had attracted law enforcement's attention (Detective, June 2022). If that happens, the user may delete potential evidence or move illegal activities on another platform – one that law enforcement would need to conduct further investigations to identify. As officers explained, "We're trying to really identify people who are harming the community," (Chief, August 2022), and "the hardest part is putting somebody behind the screen ... But you got to ... you have to put that person behind the screen and prove that they're the ones who are doing it" (Detective, May 2022). Putting someone behind the screen means locating an accountholder offline. Other investigators explained that when companies shut down victims' accounts simply because they were the subject of a search warrant, victims may also become less willing to participate in investigations – a consequence that also frustrates investigations (Agent, November 2019).

Company respondents recognized that shutting down accounts can hinder law enforcement investigations, but they viewed such actions as within their companies' authority and as the right thing to do. As the legal assistant emphasized, even if the affected user moved to another platform to continue the misconduct, the immediate problem on their services would be addressed (Legal Assistant, February 2022). Another attorney emphasized that the company undertakes these account closures as part of the enforcement of its own policies (Counsel, March 2022). Account shutdowns can thus serve as a countersignal to the practice of complying with no-notice orders. When companies comply with no-notice orders and refrain from notifying users, they signal responsiveness to legal mandates; when they independently decide to shut down accounts despite agent requests, they signal independence from law enforcement efforts – demonstrating their willingness to prioritize platform governance even when it impedes formal investigations.

Platform actors also engage in symbolic ambivalence when they navigate emergency information requests. While companies are permitted, under ECPA and CalECPA, to provide information to police in emergencies involving the danger of death or serious physical injury to a person, neither law specifies exactly which kinds of information must be provided. This silence in law permits platform actors to signal both compliance with emergency requests as well as independence in judgment about what information is needed by law enforcement. For example, an investigator may contact

a platform's LER team and ask for the IP address of a user suspected of abducting a child and the content of communications between that user and the child user. From the perspective of some platform respondents, however, "[t]here weren't that many valid business use cases or justifications for providing email content absent a search warrant"; "a lot of the emergency requests could be addressed with an IP address usually" and, if agents wanted content information beyond basic details, they could obtain legal process (Legal Assistant, February 2022). Law enforcement respondents expressed frustration with this kind of response. As one agent explained, "We all have stories about cases where we have explained why we feel like there is an immediate danger to life in a particular case and have had someone [at a company] say, 'Well, I just don't agree with you.' And I mean, that's really frustrating" (Deputy Chief, June 2022). By selectively providing only the information that company respondents deem necessary to address the emergency, platform actors signal responsiveness to the legal goal of preventing harm while simultaneously asserting their independence from law enforcement's interpretations of the necessity of such information.

Conditions shaping legitimacy assessments and symbolic ambivalence

Symbolic ambivalence does not operate as a fixed set of responses. Platform actors do not necessarily signal both independence and responsiveness in every interaction, nor do they signal each dimension equally. In some cases, for example, they may alternate between them over the course of a single demand – complying with no-notice orders but then shutting down accounts. In others, they fold both signals into the same action – providing some information in response to an emergency, while simultaneously limiting what is provided, thus signaling independence too. This section identifies organizational and legal conditions that shape how actors assess the legitimacy implications of perceived compliance as well as how they undertake practices of symbolic ambivalence in response. These conditions include: (1) the types of services or products offered by the platform, (2) the organizational responsibilities and tenure of platform actors and (3) the potential for legal liability.

At the organizational level, the nature of the platform's products and services – including their particular features – appears to be a key condition. This is because the functionalities enable users to undertake different types of conduct. For example, platforms that facilitate communication or permit user-generated content, such as social media or messaging applications, are likelier to encounter users distributing CSAM. Platforms designed for online-to-offline interactions – such as ride-hailing, network hospitality, and dating services – are likelier to facilitate in-person violence, such as robberies and sexual assaults. When platform actors worked for companies whose products facilitated crimes thought to be serious, particularly involving child exploitation and in-person violence, they were more likely to regard law enforcement demands as morally legitimate – and to assess perceived compliance as serving organizational legitimacy. In such cases, respondents expressed willingness to make exceptions to notice and shutdown policies, and to avoid the risk that targeted accountholders would be alerted and prompted to evade formal apprehension (Trust and Safety Director, April 2021; Counsel, March 2022).

Companies whose products and services facilitate financial transactions rather than user-generated content or communications may assess legitimacy differently,

prioritizing signaling responsiveness in other types of cases. As scholars have noted, fraud has been a persistent challenge in internet commerce, “immediately [giving] rise to problems of trust and social order as people were scammed or otherwise ripped off” (Fourcade and Healy 2024: 22). Respondents for companies operating online marketplaces thus prioritized reporting crimes to law enforcement in cases leading to financial loss for consumers or companies:

Often, merchant fraud results in a loss for the company. And once we can determine there’s a high probability that it [the activity] is criminal instead of a business failure, for example, we would then reach out to law enforcement and [say, for example] ... “There’s a victim in your jurisdiction of identity theft.” ... And we would then collaborate on that investigation, prepare a case report, and pretty much say, “This is why we believe this is criminal,” and try and solicit support from law enforcement to conduct the investigation. (Investigations Specialist, December 2021)

In contrast, respondents who worked for companies that do not rely on financial transactions were much less concerned about fraud as a crime. As a director for a communications platform explained, while he would make exceptions to the company’s user-notification policy in child sexual exploitation cases, he was less inclined to do so in fraud cases: “[If] this is a fraud case or this is a conspiracy-to-whatever case ... you look at the legal process, and you’re like, ‘I think that is a case where you might choose to disclose, and then you have this back and forth’” (Trust and Safety Director, April 2021). The nature of platforms’ services may thus shape the types of crimes that actors view as serious or important enough to make perceived compliance with a conscriptive demand appear less risky, thereby reducing the necessity of signaling independence.

Organizational actors’ tenure and responsibilities may also shape how they assess the legitimacy implications of perceived compliance. Early-career professionals, particularly legal assistants and newer counsel with fewer than four years in their roles, often expressed greater concerns about the privacy implications of law enforcement demands and the potential for perceived compliance to undermine organizational legitimacy. In contrast, respondents with longer tenures reported greater awareness of the variety, scale, and scope of harms that can occur on – and, at times, be facilitated by – the platforms, and were more likely to recognize how perceived compliance could support organizational legitimacy. As one attorney explained, his perspective had expanded substantially over his seven years in his role:

I came into it with this philosophical approach—“I don’t want to be that lawyer who goes into a company and just rolls over and hands over everything to government agencies without making sure that they’re following process.” And so I’ve always been super focused on process and making sure that there’s at least some process that’s underpinning requests that we’re getting and that the process fits the type of requests that are coming in ... And since [then], I realized that there’s this whole other train of thought ... which is that companies are essentially working with the criminals to hide all this information and prevent

the government from being able to get it and being able to prevent them from stopping all these bad actors. (Counsel, July 2021)

Often, those who had worked in their roles longer had broader experience, including responsibilities such as law enforcement response, trust and safety, and compliance investigations (Legal Assistant, September 2021; Legal Director, November 2021). These experiences may have given them more opportunities to interact with law enforcement and to observe the types of wrongdoing undertaken by platform users, which could help them to understand those agents' priorities for formal enforcement. This understanding, in turn, may shape how these actors assess the legitimacy implications of perceived compliance and the necessity of signaling independence.

Longer tenures also allow platform actors more opportunities to respond to – and adjust their responses to – major public events. Several respondents noted that after Edward Snowden's disclosure of national security agencies' receipt of data from internet technology and telecommunications firms, their companies had announced strict user-notice policies advocated by the Electronic Frontier Foundation. For example, a director with over ten years of experience indicated that under those post-Snowden policies, the default was to give notice to users who were subject to a compulsory demand when legally permitted (Legal Director, November 2021). Respondents reported that over time, however, they came to question whether this approach was wise: "The EFF was very aggressive about this for a while and [wanted] in every case, you should provide notice ... And then I think companies really looked at it and they were like, 'Well, should we though? ... Are we not just ensuring the destruction of evidence?' And the answer is, 'Yeah, you probably are.' So I think a lot of companies have modified'" (Trust and Safety Director, April 2021).

Interestingly, platform actors' previous professional experience did not appear to shape their assessments to the same extent. There were no substantial differences in responses between respondents who had previously worked in law enforcement, either as prosecutors or as officers, except for one manager's observation that former law enforcement experience allowed some company staff to identify when requests seemed overly broad or reflected investigative shortcuts rather than necessity, or as he put it, to see through "tricks" that agents use to get "things that they don't need as part of that investigation – that they may just be asking for because they're looking for as much data as possible, not really knowing what they need" (Safety Manager, November 2021).

The broader legal and political environment also shapes platform actors' assessments. Respondents reported that major events had shaped their views of the legitimacy of law enforcement and the potential implications of company responses. In addition to Snowden's disclosures, respondents referred to the Black Lives Matter protests and the overturning of the constitutional right to abortion established in *Roe v. Wade* (U.S. 1973) as key events that heightened their normative concerns regarding warrants and shaped their assessments of the consequences of compliance. The director explained that when demands were seen as targeting protestors, employees were more inclined to signal independence:

If [law enforcement is] looking at the protestors during the Black Lives Matter protests, you will find a lot of resistance to providing any information and a lot of either procedural objections or substantive objections that would not otherwise exist. (Trust and Safety Director, March 2021)

This response suggests that when perceived law enforcement demands appeared to target protestors – and conduct that could be viewed primarily as democratic participation – this director assessed perceived compliance as a threat to moral legitimacy. Complying with such demands, for example, could thus risk companies being seen as suppressing political speech, supporting racism, and aligning with contested state power. In such contexts, actors would have greater need to signal independence by raising “objections that would not otherwise exist,” even if the company ultimately did produce responsive data.

National and international events could also shift assessments in the other direction, leading actors to view perceived noncompliance as a greater legitimacy problem. One director identified mass shootings as moments when intense public pressure seemed to compel responsiveness:

Charlie Hebdo—that was something that a lot of companies felt like—We can’t push back on law enforcement for these types of issues ... If they feel like there’s an imminent terrorist attack ... most companies would be like, “Let’s see what we could do to help” ... because of the environment. But I think it ebbs and flows, right? Depending on how current events are going. (Legal Director, November 2021)

Another respondent discussed similar shifts in how he and his colleagues thought about compulsory demands: “I will say that Charlottesville ... the white rise of white supremacy ... I think a lot of it is just like the world has changed. And I think platforms have come around a little bit” (Trust and Safety Director, March 2021). These shifting political contexts shape both how actors assess the legitimacy implications of perceived compliance and how they adjust the signaling. In other words, when organizational actors fear that compliance could erode legitimacy, they may foreground independence. But when public pressure seems to demand visible action against particularly serious crimes, organizational actors may foreground responsiveness instead.

The potential for legal liability also shapes platform actors’ compliance practices. Failure to comply with compulsory process laws can raise the possibility of litigation in that prosecutors can then seek contempt orders from courts. In addition, laws seeking to reduce child sexual abuse and sex trafficking impose substantial fines and potential criminal and civil liability on companies. Under federal law, companies that knowingly and willfully fail to report known or suspected instances of CSAM face fines for each failure to report (18 U.S.C. § 2258A). Companies can also face criminal and civil liability for knowingly facilitating sex trafficking (Albert et al. 2021; Citron 2023). Such matters carry not only financial and legal risks but also legitimacy consequences – a greater prospect of being publicly seen as facilitating child exploitation or sex trafficking. These combined legal and reputational stakes also appear to shape actors’ assessments of legitimacy.

Indeed, platform respondents reported prioritizing responsiveness over independence signals in matters involving child exploitation and sex trafficking. One director

explained that in matters involving CSAM, he was comfortable not notifying users, even when officers had failed to obtain a no-notice order:

[C]ompanies actually exercise a lot of discretion there and they're like, "Is this a case where I want to notify [the user]?" And so, you can make that decision and you can say in child safety cases, "Even when you [law enforcement] don't come to me with a sealing order, a nondisclosure order, or even when there's no statutory basis, I'm not going to disclose because I don't want to protect these people. (Trust and Safety Director, April 2021)

Another director explained that she approached sex trafficking cases differently from cases involving sexual assault (Director, April 2022). In sexual assault cases, the company's policy was not to disclose information about the assaults to police unless the company had the survivor's consent. Thus, even if the company became aware of an alleged assault by one user against another, she would not report the incident to the police unless the survivor chose to do so. In contrast, in sex trafficking cases, she expressed willingness to directly report incidents and share data with law enforcement, regardless of consent. For this respondent and her company, the combined risk of financial, legal, and reputational liability may have shifted assessments of perceived compliance – and perceived noncompliance – toward signaling responsiveness over independence.

The prioritization of signaling responsiveness in such cases does not necessarily mean that actors abandon practices of symbolic ambivalence. Even in matters involving child sexual abuse material, platform actors may still seek to signal independence. For example, federal law does not specify which data must be included when companies submit CyberTips to NCMEC – only which data are permitted to be provided. Law enforcement respondents explained that while some companies provide detailed information – including confirmation that images found by the provider are a known image of child sexual abuse image – others provide so little that it was difficult to understand what circumstances even prompted the company to submit a CyberTip (Deputy Chief, June 2022). Such variation may reflect different assessments of the legitimacy implications of compliance. Companies that provide detailed reports can signal not only an obligation to fulfill reporting requirements but also a greater alignment with law enforcement objectives regarding enforcing laws that prohibit child exploitation. In contrast, companies providing minimal reports can signal both compliance – fulfilling their legal reporting mandate – and independence – providing what is minimally required. That symbolic ambivalence persists even in these cases is notable: child exploitation and sex trafficking represent criminal conduct that shares broader social consensus than many other crimes. The relative consensus around these crimes, combined with the possibility of substantial legal exposure, creates strong pressures toward signaling responsiveness. Yet, as the variation in CyberTip reporting suggests, platform actors still have ways to signal independence.

Before turning to the conclusion, I note two limits of my findings. First, the majority of company respondents in my sample worked for larger companies with more than 1,000 employees offering particular types of products or services. As such, these findings cannot be generalized to all online platform companies. However, the results offer analytically useful starting points for understanding these conditions because

larger, consumer-facing organizations are more likely to face the legitimacy dilemma that gives rise to symbolic ambivalence. In contrast, smaller or less visible firms may be able to comply more straightforwardly without navigating the same tensions.

Second, like other neoinstitutional studies of law, this analysis has focused on compliance signaling rather than substantive compliance. In the instant case, assessing whether platforms' compliance efforts actually achieve substantive compliance may be impossible for company outsiders, given the opacity of both criminal investigations and companies' data holdings (Fang 2024). As such, the activities through which platform actors undertake symbolic ambivalence are the very same activities through which they either substantively realize legal demands or fail to do so. The symbolic and substantive dimensions of compliance are inseparable in practice, even as they operate as distinct dimensions of organizational responses to law.

Conclusion

This study's examination of how platform actors navigate contested law suggests an important extension to neoinstitutional theories of law. A central insight of this literature is that organizational responses to law have a symbolic component – a signaling dimension that operates independently of whether those responses substantively achieve the law's aims (Edelman 2016; Talesh 2009, 2012). Building on this insight, existing studies have focused on explaining how perceived compliance with law can help organizations to maintain legitimacy – in particular, on how symbolic compliance can signal organizations' attention to a law's aims, even when those compliance practices do not necessarily achieve those aims substantively. This article extends neoinstitutional theory by showing that the relationship between perceived compliance and legitimacy is contingent rather than straightforward. In particular, it shows how symbolic compliance is one specific form of compliance signaling – one that may be the more typical response when organizations navigate laws whose aims enjoy relatively strong social consensus. When laws lack such consensus, however, organizations encounter a more complex legitimacy dilemma to which symbolic ambivalence may constitute a more typical set of responses.

This study also contributes to studies of platform governance by shedding light on how platform actors manage organizational legitimacy. Existing work has documented companies' use of various legitimacy strategies, including developing private governance systems that draw on legal principles and forms (Bloch-Wehba 2019; Gillespie 2018; Klonick 2018) and establishing collaborative arrangements with civil society and other government bodies (Caplan 2023). This study identifies symbolic ambivalence as complementary practices within this repertoire – one that permits organizations to navigate contested laws where perceived compliance itself carries conflicting legitimacy implications. By signaling both responsiveness to and independence from contested law, symbolic ambivalence allows platforms to manage competing legitimacy assessments, particularly for large, consumer-facing organizations whose visibility intensifies potential audience scrutiny.

Several questions remain for future research. First, what mechanisms translate individual actors' compliance practices and assessments of particular demands into company-level response patterns? My findings reveal that organizational actors can hold genuinely crosscutting assessments of the legitimacy implications of perceived

compliance that shape their subsequent compliance practices, yet the mechanisms through which these individual-level assessments and practices become institutionalized remain unclear. What formal mechanisms – such as case management systems, internal guidelines, performance metrics, or managerial review processes – channel worker-level assessments and practices into organizational policies and procedures? Understanding these mechanisms could clarify not only how platform companies' broader strategies draw on the legitimacy assessments and compliance practices of LER and T&S staff but also how organizational structures and policies may shape or constrain those actors' assessments and responses.

Second, how does the selective visibility of compliance practices enable platforms to signal multiple claims to multiple audiences? My study focused primarily on how platform actors understand the legitimacy implications of perceived compliance with contested law and manage those tensions through practices of symbolic ambivalence. While these practices may be visible to some law enforcement agents who interact with companies, many may remain opaque to other audiences, including consumers, privacy advocates, other platform companies, regulators, and even less experienced agents. This raises an important question about the scope conditions of symbolic ambivalence as a legitimacy strategy: Does symbolic ambivalence depend on selective visibility across audiences? For instance, privacy advocates may become aware of user-notification practices through litigation, interpreting them as signals of the platform's commitment to user protection, whereas law enforcement agents may interpret actors' compliance in domains such as CSAM investigations as signals of the platform's responsiveness to investigative and public safety aims. Because few audiences see the full pattern of compliance practices, platforms can signal multiple, sometimes conflicting claims. Future research should examine whether and how symbolic ambivalence operates when compliance practices become more consistently visible to multiple audience groups.

This study also raises questions beyond the case of online platform companies. In particular, how do organizations in legally settled fields renegotiate their relationships with laws and legal institutions in the face of events that challenge the legitimacy of those laws and institutions? Edelman's conceptualization of symbolic compliance emerged from her study of organizational responses to employment discrimination law during a period when, despite business resistance to specific mandates, the basic legitimacy of civil rights aims was more broadly accepted. Today, however, the legitimacy of many laws and legal institutions lack such consensus. Antidiscrimination law itself is much contested again. As the legitimacy dilemmas created by contested laws grow in increasingly fragmented social and political environments, compliance practices that signal both responsiveness to legal aims and independence from them may become a more frequent and important feature of organizational responses to law.

Acknowledgements. I would like to thank the *Law & Society Review* editors and anonymous reviewers, as well as Calvin Morrill, Rachel Stern, Paul Schwartz, Michelle Phelps, Paulo Barrozo, Aziz Rana, and commentators and participants at the Empirical Criminal Law Roundtable, the Junior Faculty Forum for Law and STEM, the Culp Colloquium, the Privacy Law Scholars Conference, the Consumer Law Scholars Conference, the Information Society Project Ideas Lunch, the Law and Technology Workshop, and the Junior Faculty Roundtable at Boston College Law School for their generosity and feedback. I am also indebted to Lauren Edelman for her support of this project. Finally, I am grateful to the interview respondents who shared their time and experiences with me. Any errors are my own.

Financial support. This material is based upon research supported by the Law and Science Dissertation Grant Program administered by Arizona State University under National Science Foundation SBE No. 2016661, as well as the Center for the Study of Law and Society and the Center for Long-Term Cybersecurity at the University of California, Berkeley.

Conflict of interests. The author declares none.

References

- Adediran, Atinuke O. 2026. *Disclosureland: How Corporate Words Constrain Racial Progress*. Cambridge: Cambridge University Press.
- Albert, Kendra, Emily Armbruster, Elizabeth Brundige, et al. 2021. "FOSTA in Legal Context." *Columbia Human Rights Law Review* 52 (3): 1084–158.
- Ayling, Julie and Peter Grabosky. 2006. Policing By Command: Enhancing Law Enforcement Capacity Through Coercion. *Law & Policy* 28 (4): 420–43.
- Ball, Kirstie, Ana Canhoto, Elizabeth Daniel, Sally Dibb, Maureen Meadows, and Keith Spiller. 2015. *The Private Security State?: Surveillance, Consumer Data and the War on Terror*. Copenhagen: CBS Press.
- Barbrook, Richard and Andy Cameron. 1996. "The Californian Ideology." *Science as Culture* 6 (1): 44–72.
- Bardach, Eugene and Robert A. Kagan. 1982. *Going by the Book: The Problem of Regulatory Unreasonableness*. Philadelphia: Temple University Press.
- Bartley, Tim and Curtis Child. 2011. Movements, Markets and Fields: The Effects of Anti-Sweatshop Campaigns on U.S. Firms, 1993–2000. *Social Forces* 90 (2): 425–51.
- Bartley, Tim and Curtis Child. 2014. "Shaming the Corporation: The Social Production of Targets and the Anti-Sweatshop Movement." *American Sociological Review* 79 (4): 653–79.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and Rob BJ Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44.
- Bender, David. 2025. *Computer Law: A Guide to Cyberlaw and Data Privacy*, 51.03. Vol. 6. New York: Matthew Bender.
- Bloch-Wehba, Hannah. 2019. "Global Platform Governance: Private Power in the Shadow of the State." *SMU Law Review* 72 (1): 27–80.
- Bloch-Wehba, Hannah. 2021. "Content Moderation as Surveillance." *Berkeley Technology Law Journal* 36 (3): 1297–340.
- Boustead, Anne E. 2016. "Police, Process, and Privacy: Three Essays on the Third Party Doctrine." Ph.D. diss., The Pardee RAND Graduate School.
- Boyd, Josh. 2002. "In Community We Trust: Online Security Communication at eBay." *Journal of Computer-Mediated Communication* 7 (3): JCMC736.
- Brayne, Sarah. 2014. "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment." *American Sociological Review* 79 (3): 367–91.
- Brayne, Sarah, Sarah Lageson and Karen Levy. 2023. "Surveillance Deputies: When Ordinary People Surveil for the State." *Law & Society Review* 57 (4): 462–88.
- Byrne, John J. 1993. The Bank Secrecy Act: Do Reporting Requirements Really Assist the Government. *Alabama Law Review* 44 (3): 801–38.
- California Department of Justice Data Portal. 2016–2020. <https://openjustice.doj.ca.gov/data> (accessed February 8, 2026).
- Caplan, Robyn. 2023. Networked Platform Governance: The Construction of the Democratic Platform. *International Journal of Communication* 17: 3451–72.
- Cardozo, Nate, Kurt Opsahl and Rainey Reitman. 2016. "Who Has Your Back? Protecting Your Data From Government Requests: Sharing Economy Edition." Electronic Frontier Foundation. <https://perma.cc/3H7L-MP2W> (accessed February 8, 2026).
- Chiarello, Elizabeth. 2015. "The War on Drugs Comes to the Pharmacy Counter: Frontline Work in the Shadow of Discrepant Institutional Logics." *Law & Social Inquiry* 40 (1): 86–122. doi:10.1111/lsi.12092.
- Chiarello, Elizabeth. 2023. "Trojan Horse Technologies: Smuggling Criminal-Legal Logics into Healthcare Practice." *American Sociological Review* 88 (6): 1131–60.

- Chiarello, Elizabeth. 2024. *Policing Patients: Treatment and Surveillance on the Frontlines of the Opioid Crisis*. Princeton, NJ: Princeton University Press.
- Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press.
- Citron, Danielle Keats. 2023. "How to Fix Section 230." *Boston University Law Review* 103 (3): 713–61.
- Citron, Danielle Keats and Ari Ezra Waldman. Forthcoming. "The Evolution of Trust and Safety." *Emory Law Journal*.
- Cohen, Julie E. 2019. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York: Oxford University Press.
- Collier, Ruth Berins, V. B. Dubal and Christopher L. Carter. 2018. "Disrupting Regulation, Regulating Disruption: The Politics of Uber in the United States." *Perspectives on Politics* 16 (4): 919–37. doi:[10.1017/S1537592718001093](https://doi.org/10.1017/S1537592718001093).
- Cullen, Olivia, Keri Zug Ernst, Natalie Dawes, Warren Binford and Gina Dimitropoulos. 2020. "'Our Laws Have Not Caught up with the Technology': Understanding Challenges and Facilitators in Investigating and Prosecuting Child Sexual Abuse Materials in the United States." *Laws* 9 (4): 4. doi:[10.3390/laws9040028](https://doi.org/10.3390/laws9040028).
- Deephouse, David L. 1996. "Does Isomorphism Legitimate?." *Academy of Management Journal* 39 (4): 1024–39.
- Denyer Willis, Graham. 2023. "'Trust and Safety': Exchange, Protection and the Digital Market-Fortress in Platform Capitalism." *Socio-Economic Review* 21 (4): 1877–95. doi:[10.1093/ser/mwad003](https://doi.org/10.1093/ser/mwad003).
- DiMaggio, Paul J. and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48 (2): 147–60.
- Douek, Evelyn. 2022. "Content Moderation as Systems Thinking." *Harvard Law Review* 136 (2): 526–607.
- Dvoskin, Brenda and Thomas Kadri. Forthcoming. "Safe Sex in the Age of Big Tech Feminism." *Harvard Journal of Law and Technology*.
- Edelman, Lauren B. 1990. "Legal Environments and Organizational Governance: The Expansion of Due Process in the American Workplace." *American Journal of Sociology* 95 (6): 1401–40. doi:[10.1086/229459](https://doi.org/10.1086/229459).
- Edelman, Lauren B. 1992. "Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law." *American Journal of Sociology* 97 (6): 1531–76. doi:[10.1086/229939](https://doi.org/10.1086/229939).
- Edelman, Lauren B. 2016. *Working Law: Courts, Corporations, and Symbolic Civil Rights*. Chicago: University of Chicago Press.
- Edelman, Lauren B. and Mark C. Suchman. 1997. "The Legal Environments of Organizations." *Annual Review of Sociology* 23: 479–515. doi:[10.1146/annurev.soc.23.1.479](https://doi.org/10.1146/annurev.soc.23.1.479).
- Edelman, Lauren B., Christopher Uggen and Howard S. Erlanger. 1999. "The Endogeneity of Legal Regulation: Grievance Procedures as Rational Myth." *American Journal of Sociology* 105 (2): 406–54. doi:[10.1086/210316](https://doi.org/10.1086/210316).
- Electronic Frontier Foundation. 2011. "Who Has Your Back?" <https://perma.cc/KZA6-BPLE> (accessed February 8, 2026).
- Electronic Frontier Foundation. 2012. "Who Has Your Back? 2012." <https://perma.cc/JZ9R-DDMR> (accessed February 8, 2026).
- Electronic Frontier Foundation. 2013. "Who Has Your Back? 2013." <https://perma.cc/XM58-DEL3> (accessed February 8, 2026).
- Electronic Frontier Foundation. 2014. "Who Has Your Back? Government Data Requests 2014." <https://perma.cc/8RTF-8UDU> (accessed February 8, 2026).
- Electronic Frontier Foundation. 2015. "Who Has Your Back? Government Data Requests 2015." <https://perma.cc/MZR3-XC7H> (accessed February 8, 2026).
- Fang, Yan. 2024. "Internet Technology Companies as Evidence Intermediaries." *Virginia Law Review* 110 (5): 1227–313.
- Farid, Hany. 2018. "Reining in Online Abuses." *Technology and Innovation* 19 (3): 593–99.
- Fourcade, Marion and Kieran Healy. 2024. *The Ordinal Society*. Cambridge, MA: Harvard University Press.
- Freiwald, Susan. 2018. "At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)." *Berkeley Technology Law Journal* 33 (1): 131–75.
- Friedland, Roger and Robert R. Alford. 1991. "Bringing Society Back In: Symbols, Practices, and Institutional Contradictions." In *The New Institutionalism in Organizational Analysis*, edited by Walter W. Powell and Paul J. DiMaggio, 232–63. Chicago: University of Chicago Press.
- Gallagher-Mackay, Kelly. 2014. "Teachers' Duty to Report Child Abuse and Neglect and the Paradox of Noncompliance: Relational Theory and 'Compliance' in the Human Services." *Law & Policy* 36 (3): 256–89. doi:[10.1111/lapo.12020](https://doi.org/10.1111/lapo.12020).

- Gartrell, Nate and Marisa Kendall. 2017. "Uber Sanctioned for Refusing to Comply with Moraga Sexual Battery Investigation, Judge Calls Company's Record 'Horrific.'" *Mercury News*, June 23.
- Gilboy, Janet A. 1998. "Compelled Third-Party Participation in the Regulatory Process: Legal Duties, Culture, and Noncompliance." *Law & Policy* 20 (2): 135–56. doi:[10.1111/1467-9930.00045](https://doi.org/10.1111/1467-9930.00045).
- Gillespie, Tarleton. 2010. "The Politics of 'Platforms.'" *New Media & Society* 12 (3): 347–64. doi:[10.1177/1461444809342738](https://doi.org/10.1177/1461444809342738).
- Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. New Haven: Yale University Press.
- Glaser, Barney G. and Anselm L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing.
- Gray, Garry C. and Susan S. Silbey. 2014. "Governing Inside the Organization: Interpreting Regulation and Compliance." *American Journal of Sociology* 120 (1): 96–145. doi:[10.1086/677187](https://doi.org/10.1086/677187).
- Greenwood, Royston, Mia Raynard, Farah Kodeih, Evelyn R. Micelotta and Michael Lounsbury. 2011. "Institutional Complexity and Organizational Responses." *Academy of Management Annals* 5 (1): 317–71.
- Grossman, Shelby, Riana Pfefferkorn, David Thiel, Sara Shah, Renée DiResta, John Perrino, Elena Cryst, Alex Stamos and Jeffrey Hancock. 2024. *The Strengths and Weaknesses of the Online Child Safety Ecosystem*. Stanford Internet Observatory Cyber Policy Center.
- Gustafson, Kaaryn. 2009. "The Criminalization of Poverty." *Journal of Criminal Law and Criminology* 99 (3): 643–716.
- Heimer, Carol A. 1999. "Competing Institutions: Law, Medicine, and Family in Neonatal Intensive Care." *Law & Society Review* 33 (1): 17–66. doi:[10.2307/3115095](https://doi.org/10.2307/3115095).
- Jiang, Jialun "Aaron," Skyler Middler, Jed R. Brubaker and Casey Fiesler. 2020. "Characterizing Community Guidelines on Social Media Platforms." *Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing*, October 17, 287–91.
- Jonas, Anne and Jenna Burrell. 2019. "Friction, Snake Oil, and Weird Countries: Cybersecurity Systems Could Deepen Global Inequality Through Regional Blocking." *Big Data and Society* 6 (1): 1–11. doi:[10.1177/2053951719835238](https://doi.org/10.1177/2053951719835238).
- Keller, Michael H. and Gabriel J. X. Dance. 2019. "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *New York Times*, September 28.
- Kerr, Orin S. 2004. "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It." *George Washington Law Review* 72 (6): 1208–43.
- Klonick, Kate. 2018. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review* 131 (6): 1598–670.
- Kluttz, Daniel N. and Neil Fligstein. 2016. Varieties of Sociological Field Theory. *Handbook of Contemporary Sociological Theory* 185–204. Switzerland: Springer.
- Kosseff, Jeff. 2019. *The Twenty-Six Words that Created the Internet*. Ithaca: Cornell University Press.
- Lehdonvirta, Vili. 2022. *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control*. Cambridge, MA: MIT Press.
- Levi, Michael. 1991. "Regulating Money Laundering: The Death of Bank Secrecy in the UK." *British Journal of Criminology* 31 (2): 109–25. doi:[10.1093/oxfordjournals.bjc.a048093](https://doi.org/10.1093/oxfordjournals.bjc.a048093).
- Luker, Kristin. 1984. *Abortion and the Politics of Motherhood*. Berkeley, CA: University of California Press.
- Lyon, David. 2015. *Surveillance After Snowden*. Cambridge, UK: Polity Press.
- Marwick, Alice E. and Robyn Caplan. 2018. "Drinking Male Tears: Language, the Manosphere, and Networked Harassment." *Feminist Media Studies* 18 (4): 543–59. doi:[10.1080/14680777.2018.1450568](https://doi.org/10.1080/14680777.2018.1450568).
- Marx, Gary T. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.
- McPherson, Chad Michael and Michael Sauder. 2013. "Logics in Action: Managing Institutional Complexity in a Drug Court." *Administrative Science Quarterly* 58 (2): 165–96.
- Meyer, John W. and Brian Rowan. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony." *American Journal of Sociology* 83 (2): 340–63.
- Mitts, Tamar. 2025. *Safe Havens for Hate: The Challenge of Moderating Online Extremism*. Princeton, NJ: Princeton University Press.

- Musto, Jennifer, Anne E. Fehrenbacher, Heidi Hoefinger, P. G. Macioti Nicola Mai, Calum Bennachie, Calogero Giametta and Kate D'Adamo. 2021. "Anti-Trafficking in the Time of FOSTA/SESTA: Networked Moral Gentrification and Sexual Humanitarian Creep." *Social Sciences* 10 (2): 58.
- Nunn, Samuel. 2008. "Measuring Criminal Justice Technology Outputs: The Case of Title III Wiretap Productivity, 1987-2005." *Journal of Criminal Justice* 36 (4): 344-53.
- Pache, Anne-Claire and Filipe Santos. 2010. "When Worlds Collide: The Internal Dynamics of Organizational Responses to Conflicting Institutional Demands." *Academy of Management Review* 35 (3): 455-76.
- Pfefferkorn, Riana. 2022. "Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers." *Journal of Online Trust and Safety* 1 (2): 1-38. doi:10.54501/jots.v1i2.14.
- Reid, Amanda, Evan Ringel and Shanetta M. Pendleton. 2024. "Transparency Reports as CSR Reports: Motives, Stakeholders, and Strategies." *Social Responsibility Journal* 20 (1): 81-107. doi:10.1108/SRJ-03-2023-0134.
- Reitman, Rainey. 2017. "Who Has Your Back? Government Data Requests 2017." Electronic Frontier Foundation. <https://perma.cc/Q3B4-P8ZL> (accessed February 8, 2026).
- Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review* 126 (7): 1934-65.
- Rosenblat, Alex. 2018. *Uberland: How Algorithms Are Rewriting the Rules of Work*. Oakland, CA: University of California Press.
- Rozenshtein, Alan Z. 2018. "Surveillance Intermediaries." *Stanford Law Review* 70 (1): 99-190.
- Scott, W. Richard. 1998. *Organizations: Rational, Natural, and Open Systems*. 4th ed. Upper Saddle River, NJ: Prentice Hall.
- Soneji, Ananta, Vaughn Hamilton, Adam Doupé, Allison McDonald and Elissa M Redmiles. 2014. "'I Feel Physically Safe but Not Politically Safe': Understanding the Digital Threats and Safety Practices of OnlyFans Creators." *Proceedings of the 33rd USENIX Security Symposium*.
- Song, Ji Seon. 2021. "Cops in Scrubs." *Florida State University Law Review* 48 (4): 861-920.
- Song, Sarah and Irene Bloemraad. 2022. "Immigrant Legalization: A Dilemma Between Justice and the Rule of Law." *Migration Studies* 10 (3): 484-509. doi:10.1093/migration/mnac014.
- Steel, Emily. 2025. "Uber's Festering Sexual Assault Problem." *New York Times*, August 6.
- Suchman, Mark C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches." *The Academy of Management Review* 20 (3): 571-610. doi:10.2307/258788.
- Suzor, Nicolas P. 2019. *Lawless: The Secret Rules that Govern Our Digital Lives*. Cambridge: Cambridge University Press.
- Talesh, Shaubin A. 2009. "The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law." *Law & Society Review* 43 (3): 527-62.
- Talesh, Shaubin A. 2012. "How Dispute Resolution System Design Matters: An Organizational Analysis of Dispute Resolution Structures and Consumer Lemon Laws." *Law & Society Review* 46 (3): 463-96.
- Talesh, Shaubin A. 2015. "Rule-Intermediaries in Action: How State and Business Stakeholders Influence the Meaning of Consumer Rights in Regulatory Governance Arrangements." *Law & Policy* 37 (1-2): 1-31.
- Taplin, Jonathan. 2017. *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy*. New York: Little, Brown and Company.
- Thornton, Patricia H., William Ocasio and Michael Lounsbury. 2012. *The Institutional Logics Perspective: A New Approach to Culture, Structure, and Process*. Oxford: Oxford University Press.
- Timmermans, Stefan and Iddo Tavory. 2012. "Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis." *Sociological Theory* 30 (3): 167-86. doi:10.1177/0735275112457914.
- Trust & Safety Professional Association. n.d. "Introduction to Trust & Safety." Accessed December 3, 2025. <https://www.tspa.org/curriculum/ts-fundamentals/industry-overview/intro-to-ts/>.
- Tyler, Tom R. 2023. "Whither Legitimacy? Legal Authority in the Twenty-First Century." *Annual Review of Law and Social Science* 19 (1): 1-17. doi:10.1146/annurev-lawsocsci-110722-074236.
- Tyler, Tom R. and Jeffrey Fagan. 2008. "Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities Symposium." *Ohio State Journal of Criminal Law* 6 (1): 231-76.
- Tyler, Tom R., Tracey L. Meares and Matt Katsaros. 2025. "New Worlds Arise: Online Trust and Safety." *Annual Review of Criminology* 8 (1): 171-92. doi:10.1146/annurev-criminol-111523-122337.
- US Department of Justice Bureau of Justice Statistics. 2016. "Law Enforcement Agency Roster (LEAR)." *Inter-University Consortium for Political and Social Research [Distributor]*, 2017-04-05. February 8, 2026. doi:10.3886/ICPSR36697.v1.

Van Dijck, José, Thomas Poell and Martijn de Waal. 2018. *The Platform Society: Public Values in a Connective World*. New York: Oxford University Press.

Vergne, Jean-Philippe. 2012. "Stigmatized Categories and Public Disapproval of Organizations: A Mixed-Methods Study of the Global Arms Industry, 1996–2007." *Academy of Management Journal* 55 (5): 1027–52.

Verma, Anjuli. 2015. "The Law-Before: Legacies and Gaps in Penal Reform." *Law & Society Review* 49 (4): 847–82. doi:[10.1111/lasr.12163](https://doi.org/10.1111/lasr.12163).

Waldman, Ari Ezra. 2021. *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge: Cambridge University Press.

Weber, Steven. 2019. *Bloc by Bloc: How to Build a Global Enterprise for the New Regional Order*. Cambridge, MA: Harvard University Press.

Wexler, Rebecca. 2014. "Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders." *Yale Law Journal Forum* 124: 158–79.

Zittrain, Jonathan. 2023. "'We Don't Know What We Want': The Tug between Rights and Public Health Online." *Duquesne Law Review* 61 (2): 183–208.

Zuckerman, Ethan and Chand Rajendra-Nicolucci. 2023. "From Community Governance to Customer Service and Back Again: Re-Examining Pre-Web Models of Online Governance to Address Platforms' Crisis of Legitimacy." *Social Media + Society* 9 (3): 1–12. doi:[10.1177/20563051231196864](https://doi.org/10.1177/20563051231196864).

Appendix A. Research interviews

	Companies	Law enforcement
Research interviews	20	27
Respondent titles	Assistant, analyst, specialist: 4	Corporal, detective, agent, inspector: 16
	Counsel, engineer: 6	Commander, lieutenant, sergeant: 4
	Manager, director: 7	Chief, deputy chief: 2
	General counsel: 1	Prosecutors: 5
	Outside counsel: 2	
Respondent organizations	Companies: 12	Municipal agencies: 12
	Law firms: 2	County agencies: 3
		State agencies: 1
Organization size (employee count) ^a		Federal agencies: 2
	Fewer than 500: 0	Fewer than 10: 0
	500 to 1000: 1	10 to 20: 1
	1001 to 5000: 5	21 to 50: 7
	5001 to 10,000: 3	51 to 100: 4
	Over 10,000: 9	101 to 300: 8
		Over 300: 7

(Continued)

(Continued.)

	Companies	Law enforcement
Department size (employee count) ^b	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: 8
Method of recruitment	Cold: 7	Cold: 20
	Network: 6	Network: 3
	Niche: 3	Niche: 0
	Snowball: 4	Snowball: 4
Interview format ^c	In person: 2	In person: 8
	Phone: 2	Phone: 11
	Video: 16	Video: 8
	Written: 0	Written: 2
Recording	Recorded: 15	Recorded: 21
	Not recorded: 5	Not recorded: 6

a. The company figures do not include outside counsel respondents.

b. The company figures do not include outside counsel respondents.

c. These figures do not add up to the total numbers of research interviews because some interviews were conducted using multiple formats.

Appendix B. Company research interviews

Number of interviews	Products and services
9	Online storage, document and media hosting, email, search
3	Social media, networking, dating
6	Online market, ride-hailing, network hospitality
2	Outside counsel
20 respondents	

Appendix C. Law enforcement research interviews

Number of interviews	Agency
17	Police department
1	Sheriff's office
5	District attorney's office
1	State investigative agency
1	Federal investigative agency
2	Federal prosecution agency
27 respondents	

Appendix D. Triangulation interviews

	Companies	Law enforcement
Triangulation interviews	8	5
Method of recruitment	Cold: 0	Cold: 1
	Network: 2	Network: 3
	Niche: 5	Niche: 1
	Snowball: 1	Snowball: 0

Yan Fang is an Assistant Professor at Boston College Law School.

Cite this article: Fang, Yan. 2026. "Symbolic ambivalence: how platform companies navigate contested law." *Law & Society Review*, 60, 234–264. <https://doi.org/10.1017/lrs.2025.10087>